Seqrite
Endpoint Security Client

Seqrite Endpoint Security Client

Quick Heal Technologies (P) Ltd.
http://www.seqrite.it

Informazioni sul Copyright

Contratto di licenza Utente finale

IMPORTANTE

SI PREGA DI LEGGERE ATTENTAMENTE QUESTO CONTRATTO DI LICENZA PRIMA DI USARE QUESTO SOFTWARE.

USANDO QUESTO SOFTWARE O CLICCANDO SUL PULSANTE “ACCETTO” O INSTALLANDO IL SOFTWARE SEQRITE IN UN QUALSIASI MODO, L'UTENTE RICONOSCE E AMMETTE DI AVER LETTO, COMPRESO E ACCETTATO TUTTI I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO DI LICENZA UTENTE. SE NON SI ACCETTANO TUTTI I TERMINI E LE CONDIZIONI DI SEGUITO, NON USARE IL SOFTWARE IN ALCUNI MODO E RESTITUIRE IMMEDIATAMENTE LO STESSO O CANCELLARE TUTTE LE COPIE IN PROPRIO POSSESSO.

Questa licenza è un contratto esecutivo tra "te" [come individuo (supponendo che tu abbia compiuto 18 anni e/o con facolta' giuridica di adempiere a un contratto), o come societa' o soggetto giuridico che utilizza il software (in seguito denominato "tu" o "tuo" per brevita'), denominato licenziatario e Quick Heal Technologies Ltd (di seguito denominata “Quick Heal” per brevità). In considerazione del pagamento del Canone di Licenza, testimoniato dalla Ricevuta di pagamento, Seqrite garantisce un diritto non esclusivo e non trasferibile di usare il Software durante il Periodo di durata della Licenza. Seqrite si riserva tutti i diritti non espressamente garantiti,e ritiene il titolo e proprietà del Software, includendo tutte le copie sucessive su qualsiasi formato. Questo software e tutto il materiale scritto accompagnatorio sono di proprietà di Seqrite e sono protetti da copyright. Copia del software o del materiale scritto sono espressamente proibiti.

COSE DA FARE E COSE DA NON FARE:

E’ permesso:

- Utilizzare una copia del software su un solo computer. In caso di multi-utenti, utilizzare il software solo sul numero di sistemi indicato sulla confezione, nel certificato di licenza d’uso o nella fattura/ricevuta di acquisto.
- Effettuare una copia del software esclusivamente ai fini di backup.
- Installare il software su una rete, purché si disponga di una copia con licenza del software per ogni computer che può accedere al software su quella rete.

Non è permesso:

- Sublicenziare, affittare o noleggiare alcuna parte del software.
- Fare il debug, decompilare, disassemblare, modificare, tradurre ed effettuare il reverse engineering del software.
- Provare a fare un tentativo di svelare / scoprire il codice sorgente del software.
- Usare il software per scopi illegali e non autorizzati.

ATTIVAZIONE OBBLIGATORIA

Seqrite avverte che nel processo di installazione del software, eventuali altri prodotti / software per la sicurezza installati sul computer devono essere disinstallati o essere disabilitati se non sono compatibili con il software Seqrite. I diritti di licenza concessi ai sensi del presente Accordo sono limitati per i primi venti (20) giorni dopo la prima installazione il prodotto a meno che non si forniscano le informazioni di registrazione necessarie ad attivare la tua copia con licenza, come descritto in Attivazione guidata del Prodotto. È possibile attivare il Prodotto tramite Internet o telefono (in questo caso possono essere applicati costi da parte del fornitore dei servizi telefonici). Potrebbe anche essere necessario riattivare il prodotto, se capita di reinstallarlo per qualche motivo. Ci sono misure tecnologiche di questo prodotto, che è stato progettato per evitare che venga usato senza licenza o in modo illegale. L'utente accetta che possiamo usare tali misure. L'utente accetta che il software Seqrite può utilizzare le misure che possono controllare e prevenire la pirateria di software.

Ai sensi del presente accordo, e in assenza di incidenti, abuso o uso improprio, Seqrite garantisce al licenziatario, che il disco dove è registrato il software è privo di difetti nei materiali e nella lavorazione in condizioni d'uso normali per un periodo di trenta (30) giorni dalla data del pagamento, come evidenziato da una copia della ricevuta di pagamento. Seqrite ha il solo obbligo, come previsto dall'accordo, a propria discrezione di scegliere tra la restituzione di un importo pari al pagamento ricevuto come da copia della ricevuta/fattura, o di sostituire il disco non funzionante, il quale sarà restituito assieme alla copia della ricevuta/fattura.

COLLEGAMENTI A SITI WEB DI TERZE PARTI

Il software contiene collegamenti a siti di terse parti, come utente è possible collegarsi a tali siti come utilizzatori del software. I siti web di terse parti non sono controllati da Seqrite, e Seqrite non è responsabile del contenuto presente in tali siti, e di tutti i link contenuti nei siti web di terze parti . Seqrite fornisce collegamenti a siti di terze parti per vantaggio e non è responsabile di perdita o di danni causati da Tali siti.

SUPPORTO

Seqrite offre funzionalità di supporto durante l'utilizzo di questo software come Live Chat con il team di supporto tecnico e/o il team di supporto tecnico potrà, a tua discrezione, prendere l'accesso remoto del computer. Avvalersi di tale sostegno sarà unicamente a tua discrezione e sarai l'unico responsabile di effettuare il backup dei dati esistenti / software / programmi nel tuo computer prima di avvalerti di tale assistenza. Seqrite non potrà essere ritenuta responsabile per eventuali perdite di dati di ogni tipo, diretto / indiretto / perdita o danneggiamento di dati / danni patrimoniali durante l'intero processo. Se in qualsiasi momento, il team di supporto tecnico sarà del parere che il problema va oltre il proprio ambito, sarà discrezione di Seqrite di sospendere, interrompere o rifiutare l'assistenza così come Seqrite non dà alcuna garanzia di alcun tipo nel fornire gli elementi di supporto.

COMUNICAZIONI/EMAIL ELETTRONICHE

Una volta registrato il software mediante l'attivazione del prodotto, Seqrite può comunicare con te attraverso le informazioni di contatto presentate durante il processo di registrazione tramite e-mail o altro dispositivo elettronico di comunicazione come il telefono o un telefono cellulare. La comunicazione può essere effettuata al fine di proporre il rinnovo del prodotto o per la verifica del prodotto stesso per tuo vantaggio.

STATO AGGIORNAMENTO SEQRITE

Dopo ogni aggiornamento della copia licenziata, il modulo Seqrite Update invierà informazioni sullo stato del prodotto al Seqrite Internet Center. Le informazioni che saranno inviate al Internet Center riguardano lo stato di salute della protezione di Seqrite. Le informazioni raccolte non contengono alcu file o dato personale. Le informazioni saranno usate per garantire un supporto tecnico veloce e migliore ai clienti legittimi.

Tutti gli utenti/abbonati registrati potranno scaricare gli aggiornamenti gratuitamente a partire dalla data di attivazione della licenza fino alla data di scadenza della stessa.

RACCOLTA DELLE INFORMAZIONI

Il software di Seqrite può raccogliere le seguenti informazioni che possono/non possono contenere dati personali con o senza la tua discrezione/autorizzazione, unicamente a scopo statistico o di miglioramento e per valutare la capacità, l'efficacia e le prestazioni del prodotto di Quich Heal in materia di identificazione e/o individuazione di modelli di comportamento dannosi inerenti a siti web fraudolenti e altri rischi/minacce alla sicurezza in Internet. La password inserita dall'utente finale durante la registrazione non è memorizzata sul server Seqrite. Queste informazioni non saranno correlate con alcuna informazione personale e potranno includere, ma non limitarsi a:

- Qualsiasi tipo di file eseguibile che il Software può identificare come un potenziale modello comportamentale di malware.
- Qualsiasi tipo di informazioni relative allo stato del software sia che si sia verificato un errore durante l'installazione del software sia che l'installazione sia avvenuta con successo.
- Qualsiasi tipo di URL di siti web visitati che il software ritiene intrinsecamente e potenzialmente fraudolento.
- Qualsiasi tipo di informazioni che il software ritiene potenzialmente fraudolente, che presentano rischi/minacce per la sicurezza.
- Qualsiasi tipo di informazioni per identificare l'(MAC) Media Access Control del Dispositivo e/o il Global Positioning System (GPS) su cui il Software è stato installato.
- Qualsiasi tipo di informazioni per identificare l'Internet Protocol (IP) e le informazioni necessarie per l'efficace amministrazione delle licenze e per migliorare la funzionalità e l'usabilità del prodotto.
- Tu autorizzi che le informazioni / i dati come sopra raccolti possano essere utilizzati per analizzare, prevenire e individuare i potenziali rischi per la sicurezza Internet, per la pubblicazione di qualsiasi tipo di dati/relazioni/presentazioni sulle tendenze raccolte, condividendo i dati per creare consapevolezza con qualsiasi altra organizzazione e produttore.

RINUNCE

Questo pacchetto software è fornito come tale, senza alcun tipo di garanzia, espressa o implicita, compreso ma non limitato alle garanzie implicite di commerciabilità del pacchetto. In nessun caso Seqrite o i suoi fornitori saranno responsabili nei vostri confronti o di chiunque altro per eventuali danni derivanti direttamente / indirettamente o consequenziali, tra cui la perdita di dati, perdita di profitti o qualsiasi altro danno dei dati / cose derivanti dall'uso o dall'incapacità di utilizzo di questo pacchetto software.

Seqrite si riserva il diritto di cooperare in ogni procedimento legale e di fornire documenti e/o informazioni relative al tuo utilizzo del Software Seqrite.

Le esclusioni e le limitazioni di cui sopra si applicano indipendentemente dal fatto che si accetta il software.

TUTTE LE DISPUTE SONO SOGGETTE ALLA GIURISTIZIONE DI PUNE (INDIA).

Informazioni su questo documento

Questa Guida per l'Utente contiene tutte le informazioni su come installare e come utilizzare i prodotti Seqrite sui sistemi operativi Windows nel più semplice modo possibile. Ci siamo assicurati che tutti i dettagli forniti in questa guida siano aggiornati con i più recenti miglioramenti del prodotto.

L'elenco seguente descrive le convenzioni che abbiamo seguito per preparare questo documento.

Convenzione	Significato
Grassetto	Tutto evidenziato in grassetto indica che si tratta di un titolo, di un titolo della finestra, una casella di controllo o una casella a discesa, didialogo, nomi dei pulsanti, collegamenti ipertestuali, e così via.
	Questo simbolo indica la presenza di informazioni aggiuntive o importanti informazioni sull'argomento trattato.
<Passo 1> <Passo 2>	Le istruzioni indicate nell'elenco numerato indica le azioni da eseguire.

Tabella di Comparazione Seqrite Endpoint Security

Caratteristiche	**Seqrite Endpoint Security**	
	Business	**Total**
Web Security	X	✓
Protezione Spam	X	✓
Protezione Navigazione	✓	✓
Antiphishing	✓	✓
Firewall	✓	✓
IDS/IPS	✓	✓
Controllo Applicazioni	X	✓
Controllo Dispositivi	X	✓
Notifica SMS	✓	✓
Tuneup	X	✓
PC2Mobile	✓	✓
Scansione Vulnerabilità	✓	✓
Monitoraggio Attività File	✓	X
Data Loss Prevention (DLP)*	X	X
Gestione Attività	✓	✓

Nota: (*) DLP è disponibile solo con il pacchetto Data Loss Prevention

Indice

Capitolo 1. Per Iniziare

Prerequisiti

Ricordare le seguenti linee guida prima di installare Seqrite Endpoint Security sul vostro sistema.

- Più prodotti antivirus installati su un unico sistema posso causare malfunzionamenti del sistema stesso. Se è installato sul sistema un qualsiasi altro programma software antivirus, è necessario rimuoverlo prima di procedere con l'installazione di Seqrite Endpoint Security.
- Chiudere tutti i programmi aperti prima di procedere con l'installazione di Seqrite Endpoint Security.
- È consigliabile mantenere un backup dei dati nel caso in cui il sistema sia stato infettato da virus.
- Seqrite Endpoint Security deve essere installato con diritti di Amministratore.

Requisiti di Sistema

Per utilizzare Seqrite Endpoint Security, il sistema deve soddisfare i seguenti requisiti minimi.

Compatibilità dei Sistemi Operativi

Sistemi Operativi	Requisiti Minimi
Windows 2000 / Windows 2000 Server	• 300 MHz Pentium (o compatibile) • 1 GB di RAM • Service Pack 4 • Internet Explorer 6
Windows XP	• 300 MHz Pentium (o compatibile) • 1 GB di RAM • Service Pack 2 o superioire
Windows Server 2003	• 300 MHz Pentium (o compatible) • 1 GB di RAM
Windows Vista	• 1 GHz Pentium (o compatibile) • 1 GB di RAM
Windows Server 2008 / Windows Server 2008 R2	• 1 GHz Pentium (o compatible) • 1 GB di RAM

Windows 7 / Windows 8/ Windows 8.1	• 1 GHz Pentium (o compatibile) • 32-bit, 512 MB di RAM • 64-bit, 1 GB di RAM
Windows Server 2012 / Windows Server 2012 R2	• 1 GHz Pentium (o compatibile) • 1 GB di RAM

Durante l'installazione, controllare i seguenti requisiti:

Requisito spazio libero sul disco

- Il requisito è applicabile a entrambi i sistemi operativi 32 bit e 64 bit a meno che non sia espressamente indicato.
- Il requisito è applicabile a tutte le versioni del sistema operativo.
- I requisiti previsti sono i requisiti minimi di sistema. Seqrite raccomanda che il sistema abbia una configurazione superiore ai requisiti minimi per ottenere migliori risultati.
- Per controllare i più recenti requisiti di sistema, visitare il sito www.seqrite.it.

Client che supportano la scansione delle e-mail

I client di posta elettronica POP3 che supportano la funzione di scansione e-mail sono i seguenti:

- Microsoft Outlook Express 5.5 o superiore
- Microsoft Outlook 2000 o superiore
- Netscape Messenger 4 o superiore
- Eudora
- Mozilla Thunderbird
- IncrediMail
- Windows Mail

Client che non supportano la scansione delle e-mail

I client di posta elettronica POP3 che non supportano la funzione di scansione e-mail sono i seguenti:

- IMAP
- AOL
- POP3s con Secure Socket Layer (SSL)
- WebMail come Hotmail e Yahoo!

- Lotus Notes

Connessioni SSL non supportate

Email Protection non supporta le connessioni e-mail crittografate che utilizzano Secure Sockets Layer (SSL).

Requisiti Seqrite Anti-Rootkit

Questa funzione non è supportata su sistemi operativi a 64 bit.

Seqrite Controllo Dispositivi

Il sistema operativo Windows 2000, non sarà in grado di bloccare altri dispositivi all'infuori dei dispositivi di memorizzazione USB.

Seqrite Auto-Protezione

- Questa funzione non è supportata su sistemi operativi Microsoft Windows 2000.
- Questa funzione è supportata per sistemi operativi Microsoft Windows XP se installato Service Pack 2 o superiore.
- Questa funzione è supportata su sistemi Microsoft Windows Server 2003 se installato Service Pack 1 o superiore.

Seqrite PC2Mobile Scan

- Questa funzione non è supportata su sistemi operativi Microsoft Windows 2000.
- Per Windows Mobile, deve essere installato Microsoft Active Sync 4.0 o superiore.
- Per la lista dei dispositivi mobili supportati consultare: http://www.quickheal.co.in/pc2mobile.asp.

Seqrite Browser Sandbox

- Questa funzione non è supportata da sistemi operativi Microsoft Windows 2000, Microsoft Windows XP 64-bit.

Installazione e disinstallazione Endpoint Security

La distribuzione di Endpoint Security può essere gestita tramite console QHEPS.

Per sapere come installare o disinstallare il Client Endpoint Security, fare riferimento al Capitolo 2 della Guida Amministratore Seqrite Endpoint Security 6.0.

Capitolo 2. Seqrite Endpoint Security Dashboard

La Dashboard di Seqrite funge da interfaccia chiave per tutte le funzioni di Seqrite Endpoint Security. È inoltre possibile accedere alla Dashboard e ad alcune funzioni di Seqrite Endpoint Security dalla barra delle applicazioni del sistema. Seqrite protegge l'intero sistema, anche con le impostazioni predefinite. È possibile avviare Seqrite per verificare lo stato di protezione Seqrite, eseguire manualmente la scansione, visualizzare i report e aggiornare il prodotto.

È possibile avviare manualmente Seqrite in uno dei seguenti modi:

- Selezionare **Start > Programmi > Seqrite Endpoint Security > Seqrite Endpoint Security**.
- Sulla barra delle applicazioni, fare doppio clic sull'icona **Seqrite Endpoint Security** o clic con il tasto destro sull'icona **Seqrite Endpoint Security** e selezionare **Apri Seqrite Endpoint Security**.
- Selezionare **Start** > **Esegui**, digitare **Scanner** e premere **Invio** sulla tastiera.

Seqrite Endpoint Security Dashboard

La Dashboard Seqrite Endpoint Security è la finestra principale dove si può accedere a tutte le funzioni. La Dashboard è divisa in varie opzioni. La parte superiore contiene il menù del prodotto, la parte centrale contiene le opzioni di protezione e la parte inferiore contiene le funzionalità più consultate di Seqrite Endpoint Security.

Le opzioni di protezioni includono Files & Cartelle, Email, Internet & Network, e Drive Esterni & Dispositivi. Con queste opzioni, è possibile proteggere il sistema per evitare che malware e virus si infiltrino in esso.

File & Cartelle	Permette di proteggere i file e le cartelle dalle minacce nocive. Con File & Cartelle, è possibile configurare le impostazioni di scansione, la Protezione Virus, il DNAScan, il Blocco dei file, la Scansione automatica Rogueware, La scansione pianificata, Escludi file e cartelle, la Quarantena & Backup.
Email	Consente di configurare la Protezione Email, i client mail attendibili e la Protezione Anti-Spam.
Internet & Network	Consente di configurare le impostazioni per Internet e rete. Con questa opzione, è possibile configurare la Protezione Firewall, la Protezione Navigazione, la Protezione Malware, la Protezione Antiphishing, Browser Sandbox, Alert News e IDS / IPS.

Unità esterne & Dispositivi	Consente di configurare la protezione per le unità esterne. È possibile configurare la Protezione Autorun (esecuzione automatica), la scansione delle unità esterne, il Controllo Dispositivi per la protezione da furto dei dati e la scansione di dispositivi Windows Mobile.

La seconda sezione comprende i menu che consentono di configurare le impostazioni generali di Seqrite e strumenti per prevenire l'infezione da virus. È possibile fare la diagnosi del sistema e visualizzare i report delle varie attività, delle funzioni e accedere a Guida e dettagli della licenza.

Impostazioni	Permette di personalizzare funzioni come Aggiornamento automatico, Impostazioni Internet, Ripristino del Registro di Sistema, Self Protection, Protezione Password, Impostazioni Rapporti, il Report Statistiche Virus e di ripristinare le impostazioni predefinite.
Opzioni	Permette la diagnosi del sistema in caso di attacchi di virus, ripristinare le impostazioni di Internet Explorer modificate da malware, isolare i file infetti e sospetti, rimuovere roguewares e prevenire dalle infezioni delle unità USB contro le infezioni di malware autorun. È inoltre possibile escludere file dalla protezione antivirus.
Report	Permette di visualizzare i report di attività di Scansione, Protezione Virus, protezione e-mail, Pianificazione delle scansioni, Aggiornamento rapido, la scansione di memoria, Protezione dal phishing, Ripristino del Registro di sistema, Scansione all'avvio, scansione antimalware, Protezione malware, Sicurezza internet, IDS / IPS, Protezione Navigazione, Scansione PC2Mobile.
Aiuto	Permette di accedere Aiuto per Seqrite Endpoint Security, visualizzare i dettagli relativi versione del prodotto, del database dei virus, i dettagli di validità, i dettagli della licenza e cercare il supporto tecnico.

La sezione inferiore comprende le seguenti opzioni.

News	Visualizza le ultime notizie da Seqrite. È possibile visualizzare tutte le notizie facendo clic su **Visualizza tutto**.

Scansione	Fornisce varie opzioni di scansione quali scansione completa del sistema, Scansione personalizzata, la scansione di memoria, scansione all'avvio e scansione di dispositivi mobili.
Supporto	Permette di usufruire del sistema di supporto disponibile in **Supporto**.
Like	Link a Seguici su Facebook.

Opzioni del menu di destra

L'icona Seqrite Endpoint Security nella barra delle applicazioni consente di accedere e utilizzare alcune delle funzionalità importanti che sono le seguenti:

Apri Seqrite	Permette di avviare Seqrite Endpoint Security.

Endpoint Security	
Apri AntiMalware	Permette di avviare Seqrite AntiMalware.
Abilita / Disabilita Modalità Silenziosa	Consente di Attivare / Disattivare le notifiche.
Secure Browse	Permette dia attivare il browser predefinito in Sandbox per una navigazione sicura.
Abilita / Disabilita Protezione Virus	Consente di Abilitare / Disabilitare Seqrite Virus Protection.
Roaming Client	Consente di aggiornare Seqrite anche se non si è connessi alla rete aziendale.
Supporto Remoto	Consente di lanciare il software di supporto remoto.
Aggiorna ora	Consente di aggiornare Seqrite Endpoint Security.
Scansione della memoria	Consente di eseguire la scansione della memoria di sistema.

Esecuzione della Scansione Manuale

Se la protezione virus è abilitata con le impostazioni predefinite, non è necessaria una scansione manuale in quanto il sistema è costantemente monitorato e protetto. Tuttavia è possibile eseguire la scansione manuale di computer, unità, unità di (unità mappate), chiavette USB,cartelle o files a seconda delle necessità. Anche se le impostazioni predefinite per la scansione manuale sono di solito sufficienti, è possibile modificare le opzioni per la scansione manuale selezionando **File & Cartelle** > **Impostazioni Scansione** dalla schermata princiapale della Dashboard.

Esecuzione della Scansione totale del sistema

Con la scansione totale di sistema, è possibile sottoporre a scansione tutti i settori di boot, unità, cartelle e files nel computer (escluse unità di rete mappate) nel seguente modo:

- Nella schermata principale di Seqrite, Selezionare **Scansione > Scansione totale di sistema**.

  La scansione inizierà.

  Dopo il completamento della scansione, è possibile visualizzare il report, nel menù Report.

Esecuzione della Scansione Personalizzata

Con la scansione personalizzata, è possibile sottoporre a scansione file specifici o cartelle nel seguente modo:

1. Nella schermata principale di Seqrite, selezionare **Scansione** > **Scansione Personalizzata**.

   Viene vissualizzata la schermata delle preferenze di scansione personalizzata.

2. Fare clic su **Aggiungi** per individuare il percorso della cartella che si desidera sottoporre a scansione. È possibile selezionare più cartelle per la scansione e quindi fare clic su **Avvia scansione**.

   La scansione inizierà.
   Dopo il completamento della scansione, è possibile visualizzare il report, nel menù Report.

Esecuzione Scansione della memoria

Con la scansione della memoria, è possibile sottoporre a scansione la memoria nel seguente modo:

1. Nella schermata principale di Seqrite, selezionare **Scansione** > **Scansione memoria**.

   La scansione inizierà.

2. Dopo il completamento della scansione, è possibile visualizzare il report nel menù Report.

Esecuzione Scansione all' avvio

La scansione all'avvio è molto utile per disinfettare il sistema nel caso in cui il sistema sia gravemente infettato da virus che non possono essere puliti perché il sistema è attivo. Tuttavia, questa scansione viene eseguita all'avvio successivo mediante avvio di Windows NT Shell. Per attivare la scansione all'avvio, seguire la seguente procedura:

1. Nella schermata principale di Seqrite, Selezionare **Scansione** > **Scansione all'avvio di sistema**.
2. Verrà visualizzata una schermata con le modalità di avvio della scansione. Selezionare una qualsiasi delle modalità per la scansione all'avvio prima di procedere.
3. Per eseguire immediatamente la scansione del sistema, fare clic su **Si** per riavviare il sistema. Per eseguire la scansione del sistema al riavvio successivo fare clic su **No**.

Esecuzione Scansione dispositivo Mobile

1. Nella schermata principale di Seqrite, selezionare **Scansione** > **Scansione Mobile**.
2. Selezionare dalla lista il telefono mobile.

   La scansione inizierà.

3. Dopo il completamento della scansione, è possibile visualizzare il report nel menù Report.

Capitolo 3.

Centro Protezione Seqrite

Seqrite Protection Center è l'interfaccia immediata alle impostazioni di protezione che possono influenzare file, cartelle, e-mail, e così via. Permette di configurare le regole di protezione contro i virus che cercano di infiltrarsi nel sistema attraverso Internet, unità esterne, ed email. Seqrite Protection Center è suddiviso in varie sezioni. La parte superiore del centro di protezione agisce3come un indicatore di stato di sicurezza con codice colore che indica lo stato della sicurezza. Ogni icona colorata indica un'azione associata che deve essere eseguita dall' utente.

La tabella seguente indica i colori e le azioni da eseguire.

Rosso		Indica che Seqrite Endpoint Security non è configurato con le impostazioni ottimali ed è necessaria attenzione immediata. L'azione corrispondente al messaggio deve essere eseguita immediatamente per garantire la protezione del sistema.
Verde		Indica che Seqrite Endpoint Security è configurato con le impostazioni ottimali e che il sistema è protetto.
Giallo		Indica che una funzione di Seqrite Endpoint Security ha bisogno di attenzione al più presto.

Seqrite Protection Center fornisce inoltre diverse categorie di protezione e impostazioni personalizzabili. Queste categorie sono aree o mezzi attraverso i quali i malware sono in grado di avere accesso e di infettare il sistema.

Ciascuna di queste categorie visualizza funzionalità vitali che devono essere sempre tenute attivate. Se si disattiva una di queste funzionalità, l'icona della categoria corrispondente diventa di colore rosso. Le categorie e le loro funzionalità corrispondenti che sono visualizzate sull'interfaccia pricipale sono le seguenti.

File & Cartelle	Impostazioni Scansione, Protezione Virus, DNA Scan, Quarantena & Backup
Email	Protezione Email, Protezione Spam
Internet & Network	Protezione Firewall, Protezione Phishing, Browser Sandbox
Unità Esterne & Dispositivi	Protezione Autorun, Scansione unità esterne, Controllo Dispositivi

File & Cartelle

Con File & Cartelle, è possibile impostare regole di scansione per file e cartelle presenti nel sistema. È possibile impostare le regole di protezione con le seguenti impostazioni.

Impostazioni Scansione

Con Impostazioni Scansione, è possibile impostare l'avvio della scansione del sistema e le azioni da intraprendere quando viene rilevato un virus. Tuttavia, le impostazioni predefinite sono ottimali perché assicurano la necessaria protezione al sistema.

Per configurare le impostazioni di scansione, seguire questi passaggi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata di impostazione dettagli di file e cartelle.
3. Fare clic su **Impostazioni Scansione**.
4. In **Seleziona modalità scansione**, selezionare **Automatica (Raccomandata)** per iniziare la scansione automatica, o selezionare **Avanzata** per un livello di scansione avanzato.
5. In 'Seleziona un'azione da eseguire quando viene rilevato un virus', selezionare un'azione appropriata.
6. Se si desidera effettuare un backup dei file o delle cartelle prima di effettuare qualsiasi azione, selezionare **Effettua un backup prima di agire**.
7. Per salvare le impostazioni, fare clic su **Salva Modifiche**.

Selezionare modalità di scansione

Automatica (Raccomandata): la scansione automatica è il tipo scansione predefinita raccomandata in quanto garantisce la protezione ottimale che il sistema richiede. Questa impostazione è la scelta ideale per gli utenti inesperti.

Avanzata: il tipo di scansione avanzata consente di personalizzare il comportamento della scansione. Questo modalità è ideale per gli utenti esperti. Quando si seleziona l'opzione 'Avanzata', si attiva il pulsante di configurazione ed è possibile configurare le impostazioni avanzate per la scansione.

Azioni da eseguire quando viene rilevato un virus

Ripara	Se viene trovato un virus durante la scansione, ripara il file o viene messo automaticamente in quarantena se non è possibile ripararlo. Quando la scansione è terminata, appare una finestra con un riepilogo che fornisce i dettagli su tutte le azioni intraprese e tutti i dettagli della scansione. Se i file infetti sono Backdoor,

	Worm, Trojan, o Malware vengono cancellati automaticamente da Seqrite Endpoint Security .

Elimina	Elimina file infetti da virus senza avvisare l'utente. Quando la scansione è terminata,viene visualizzata una finestra di riepilogo che fornisce tutti i dettagli sulle azioni intraprese e altri dettagli di scansione.Una volta che i file sono cancellati non possono essere recuperati.
Salta	Se questa opzione è selezionata i file vengono sottoposti a scansione, ma non si interviene sui file infetti e vengono saltati. Selezionare questa opzione se non si vuole intraprendere alcuna azione quando viene rilevato un virus. Quando la scansione è terminata appare un report con tutti i dettagli della scansione.
Backup prima di effettuare azioni	Lo scanner mantiene una copia di backup dei file infetti prima di disinfettarli.I file memorizzati nel backup possono essere ripristinati dal menu quarantena.

Configurazione modalità di scansione avanzata

Per configurare la modalità di scansione avanzata, seguire questi passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata delle impostazioni di File & Cartelle.
3. Fare clic su **Impostazioni Scansioni**.
4. In 'Seleziona modalità di scansione', selezionare **Avanzata**.

   Si attiverà il pulsante di configurazione.
5. Fare clic su **Configura**.

   Viene visualizzata la schermata delle impostazioni avanzate.
6. In 'Seleziona oggetto da sottoporre a scansione', selezionare **Scansione dei file eseguibili** se si vuole che la scansione venga seguita solo per i file eseguibili o selezionare **Scansiona tutti i file** se si vuole sottoporre a scansione tutti i file.

   Comunque è selezionata come predefinita l'opzione di scansione dei file eseguibili.

   La scansione di tutti i file può richiedere molto più tempo, perciò questo processo di scansione può rallentare considerevolmente il sistema.
7. Selezionare uno dei seguenti oggetti per la scansione:
   - Scansione File Compressi: selezionare questa opzione se si vuole effetuare la scansione di file compressi quail file zip, file rar, ecc.
   - Scansione File a Pacchetto: selezionare questa opzione se si vuole scansionare file a pacchetto.

- Scansione mailbox: selezionare **Scansione rapida mailbox** per una scansione veloce o altrimenti **Scansione approfondita mailbox** per una scansione approfondita.

8. Fare clic su **OK**.
9. Fare clic su **Salva Modifiche** per salvare le impostazioni.

Scansione file archivio

La 'Scansione file archivio' consente di impostare delle regole di scansione dei file archivio quali file ZIP, file RAR, file CHM e così via.

Per configuare la Sscansione di file archivio, seguire la seguente procedura:

1. Selezionare **Scansione file archivio**.

   Si attiverà il pulsante di configurazione.
2. Fare clic sul pulsante **Configura**.

   Verrà visualizzata una schermata di riepilogo relativa alla scansione dei file archivio.
3. In 'Seleziona un'azione da eseguire quando viene rilevato un virus', selezionare una delle seguenti opzioni: Elimina, Quarantena, e Salta.
4. In 'Livello di scansione archivio', selezionare fino a che livello si desidera eseguire la scansione dei file e delle cartelle.
5. In 'Seleziona il tipo di archivio che deve essere sottoposto a scansione', selezionare il tipo di archivio.
6. Fare clic su **OK** per salvare le impostazioni.

Azioni da eseguire quando viene trovato un virus	
Elimina	Elimina un archivio contenente il file infetto da virus, senza notificarlo.
Quarantena	Durante la scansione, se viene rilevato un virus in un file archivio, esso verrà spostato in quarantena.
Salta	Salta i file rchivio contenenti virus senza effettuare nessuna azione.

Livello scansione archivio	Imposta un livello di scansione all'interno di un archivio. Il livello di scansione predefinito è impostato su livello 2. Tuttavia, aumentando il livello di scansione predefinito si può influenzare la velocità di scansione

Selezionare il tipo di archivio che dovrebbe essere sottoposto a scansione

In questa sezione è disponibile l'elenco dei file archivio che possono essere acquisiti durante il processo di scansione. Alcuni dei più comuni tipi di file

archivio sono selezionati tra i predefiniti ma è possibile personalizzare la scelta in base alle proprie necessità.

Seleziona Tutto	Consente di selezionare tuuti i tipi di file presenti nella lista.
Deseleziona Tutto	Consente di deselezionare tutti i tipi di file presenti nella lista.

Scansione file compressi

Con 'Scansione file compressi', la scansione esamina anche i file pacchetto. I pacchetti sono l'insieme di molti file, o la compressione di un singolo file per ridurne le dimensioni. Questi file hanno bisogno di applicazioni di terze parti per essere aperti. Queste applicazioni hanno funzionalità di compattare e scompattare.

I file compressi possono essere utilizzati per diffondere Malware o file dannosi infieme ad altri documenti. Quando tali pacchetti vengono scompattati possono causare danni al computer. Se si desidera decomprimere questi pacchetti, selezionare l'opzione **Scansione file compressi**.

Scansione Mailbox

Con 'Scansione Mailbox', è possibile sottoporre a scansione le caselle di posta di Outlook Express 5.0 e versioni successive (all'interno del file DBX). Virus come KAK, JS.Flea.B, ecc., rimangono all'interno del file DBX di Outlook Express e posso riapparire se le patch non vengono applicate a Outlook Express. Esamina anche gli allegati e-mail codificati con UUENCODE/MIME/BinHex (Base 64). 'Scansione Mailbox' è un'impostazione selezionata in modo predefinito che attiva una delle due seguenti opzioni:

Scansione rapida mailbox	Consente di saltare tutti i messaggi precedentemente scaricati e analizzare solo i nuovi messaggi. Questa opzione è selezionata come predefinita.
Scansione approfondita mailbox	Consente di sottoporre a scansione tutte le email presenti nella mailbox. Tuttavia, ciò può influire sulla velocità in base alla grandezza della mailbox.

Protezione Virus

Con Protezione Virus, è possibile monitorare continuamente il sistema da virus che potrebbero essersi infiltrati da varie fonti come allegati email, download da internet, trasferimento file, file eseguibili e così via.

Si consiglia di tenere sempre attiva la Protezione virus per mantenere il sistema pulito e protetto da eventuali minacce. Comunque, Protezione Virus è attiva per impostazione predefinita.

Per configurare Protezione Virus, seguire questi passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

Viene visualizzata la schermata delle impostazioni di File & Cartelle.

3. Impostare **ON** su ‘Protezione Virus’.
4. Fare clic su **Protezione Virus**.

   Apparirà la schermata delle impostazioni Protezione Virus.

5. Procedere come segue:
   - **Visualizzazione messaggi di avviso** – Selezionare questa opzione se si vogliono ricevere gli avvisi dei vari eventi, come ad esempio quando viene rilevato un malware. Comunque, questa opzione è selezionata come predefinita.
   - **Selezionare le azioni da eseguire quando viene rilevato un virus** – Selezionare un’azione appropriata quando un virus è stato rilevato durante la scansione.
   - **Backup Prima di qualsiasi azione**– Selezionare questa opzione se si vuole fare un backup dei file prima di eseguire un’azione sui file. I file salvati nel backup possono essere ripristinati dal menu Quarantena.
   - **Abilita suoni quando viene rilevato un virus**– Selezionare questa opzione se si vuole essere avvertiti mediante un suono quando viene rilevato un virus.
6. Fare clic su **Salva Modifiche** per salvare le impostazioni.

Azioni da eseguire quando viene rilevato un virus

Ripara	Durante la scansione se viene rilevato un virus, il file può essere riparato automaticamente o messo in Quarantena se non è riparabile.
Elinina	Elimina un file infetto senza avvisare.
Accesso negato	Impedisce l’accesso al file infetto.

Disattivare Protezione Virus

Posizionare ‘Protezione Virus**’** su **OFF** solo se strettamente necessario. Semmai, è possibile disattivare la protezione per un periodo di tempo, in modo che si riattivi in automatico. Comunque, quando si disattiva la protezione virus viene visualizzato un messaggio.

Scegliere tra le seguenti opzioni per disattivare la Protezione virus:

- Riattiva dopo 15 minuti
- Riattiva dopo 30 minuti
- Riattiva dopo 1 ora
- Riattiva al prossimo riavvio
- Disabilita permanentemente

Selezionare un’opzione e fare clic su **OK**.

Dopo aver disabilitato la Protezione virus, il colore dell’icona dell’opzione File & Cartelle sulla schermata principale passa da verde a rosso e viene visualizzato il messaggio "Il sistema non è sicuro". Se è stata selezionata una delle opzioni per la disabilitazione temporanea o dopo il successivo avvio, allora il colore dell'icona ritorna da rosso a verde dopo il determinato tempo o al successivo avvio. Se si è scelto di disabilitare la protezione in modo permanente, il colore dell’icona resta rosso fino a che la protezione virus non viene riattivata manualmente.

DNAScan

DNAScan è una tecnologia proprietaria di Seqrite per rilevare ed eliminare minacce nuove e sconosciute nel sistema. La tecnologia DNAScan cattura con successo i file sospetti con rilevazioni di molti meno falsi positivi. Inoltre il file sospetto viene copiato in quarantena prima di intraprendere qualsiasi azione.I file sospetti in quarantena possono essere inviati ai nostri laboratori di ricerca per ulteriori analisi, il che aiuta a monitorare le nuove minacce e a bloccarle in tempo. Dopo l'analisi infatti la minaccia viene aggiunta al database delle firme delle minacce che verrà fornita nei successivi aggiornamenti a tutti gli utenti.

Ogni volta che DNAScan rileva una nuova minaccia dannosa nel sistema, viene inviato un messaggio sul rilevamento, o viene richiesto l'intervento di un’azione durante la scansione della memoria se la scansione è impostata in modo predefinito. Una copia dei file sospetti viene inoltre messa in quarantena e sarà in seguito possibile inviarla ai laboratori di ricerca Seqrite. Sarà possibile inviare automaticamente o manualmente i file sospetti tramite email. L’invio ha luogo ogni volta che Seqrite Endpoint Security trova nuovi file sospetti nella cartella Quarantena. È necessario inviare ai laboratori di ricerca i nuovi file sospetti presenti in quarantena in un formato file crittografato.

Per configurare il DNAscan,seguire questi passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata delle impostazioni di File & Cartelle.
3. Attivare **DNAScan**.
4. Fare clic su ‘DNAScan’.

   Verrà visualizzata la schermata dettagli di DNAscan.
5. In ‘Seleziona file sospetti’, selezionare una delle seguenti opzioni:
   - **Non inviare file** – Selezionare questa opzione se non si vuole inviare i file ai laboratori di ricerca Seqrite.
   - **Invia File** – Selezionare questa opzione se si vogliono inviare i file sospetti. È anche possibile selezionare **Mostra notifica durante**

l'invio dei file per autorizzare l'invio dei file ai laboratory di ricerca Seqrite.

Se l'opzione 'Mostra notifica' non è selezionata, Seqrite invia i file sospetti senza avvisare.

.

LìInvio manual dei file può essere fatto attraverso la quarantena.

Blocco dei file compressi sospetti

File Compressi Sospetti consente di identificare e bloccare i file compressi sospetti. I file compressi sospetti sono i file che sono stati compressi con un elenco predefinito di programmi di compressione sospetti. Tali programmi sono per lo più utilizzati per comprimere file dannosi, i quali non appena scompattati possono causare gravi danni al computer. Si consiglia di tenere sempre questa opzione attivata in quanto impedisce la diffusione delle minacce.

Per configurare il blocco dei file compressi, seguire questi passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata delle impostazioni di File & Cartelle.
3. Attivare **Blocca file compressi sospetti.**

   Comunque, il blocco dei file compressi sospetti è abilitato come predefinito.

Scansione Automatica Rogueware

La funzione di scansione automatica dei rogueware di Seqrite Endpoint Security esegue la scansione e rimuove automaticamente i rogueware e falsi software antivirus di livello critico.

Per configurare la scansione automatica di Rogueware, seguire questi passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata delle impostazioni di File & Cartelle.
3. Abilitare **Scansione Automatica Rogueware**.

   Comunque, la scansione automatica dei Rogueware è abilitata come predefinita.

Scansione Pianificata

Con Scansione Pianificata, è possibile definire una pianificazione della scansione automatica del sistema. È possibile definire più pianificazioni di scansione in

modo che la scansione sia avviata a piacimento. Eseguire la scansione regolarmente aiuta a mantenere il sistema libero da virus e altri tipi di minacce.

Configurare la scansione pianificata

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata delle impostazioni di File & Cartelle.
3. Fare clic su **Scansione Pianificata**.

   Verrà visualizzata la schermata dettagli della scansione pianificata.
4. Per definire una nuova scansione pianificata, fare clic su **Nuovo**.
5. In 'Nome Scansione', dare un nome alla scansione.
6. In 'Frequenza scansione', selezionare un'opzione tra le seguenti in base alle proprie esigenze:

- Frequenza delle Scansioni:
  - 'Giornaliera': selezionare l'opzione giornaliera se si vuole effettuare una scansione giornaliera del proprio sistema. Tuttavia, questa opzione è selezionata come predefinita.
  - 'Settimanale': selezionare l'opzione settimanale se si vuole avviare la scansione in un determinato giorno della settimana. Quando l'opzione settimanale è selezionata, viene attivato il menu a tendina con i giorni della settimana per poter scegliere un giorno.
- Orario di scansione:
  - 'Esegui al primo avvio': selezionare questa opzione per programmare l'esecuzione della scansione al primo avvio della giornata. Quando è selezionato 'Esegui al primo avvio', non è specificato l'orario della giornata in cui può partire la scansione. La scansione avviene solo durante il primo avvio indipendentemente da che ora si avvia il sistema.
  - 'Avvio alle': selezionare questa opzione se si vuole iniziare la scansione del sistema in un determinato orario. Quando è selezionato 'Avvio alle', si attiva il menu a tendina in modo da poter scegliere una determinata ora per la scansione. Tuttavia, questa opzione è selezionata come predefinita.

    È inoltre possibile definire la frequenza di scansione, scegliendo fra un ampia gamma di opzioni personalizzabili.
- Priorita di scansione.

- ‘Alta’: Selezionare questa opzione se si vuole impostare una priorità di scansione alta.
- ‘Bassa’: Selezionare questa opzione se si vuole impostare una priorità di scansione bassa. Tuttavia, questa opzione è selezionata come predefinitat.

7. In ‘Impostazioni Scansione’, è possibile specificare la modalità di scansione, definire le impostazioni avanzate per la scansione, le azioni da eseguire quando viene rilevato un virus e se si desidera una copia di backup dei file prima di eseguire qualsiasi azione su di esse. Tuttavia, l’opzione predefinita è la più adeguata per mantenere pulito il sistema.
8. Fornire **Nome Utente** e **Password**.
9. Selezionare **Esegui sessione prima possibile se fallita**, per iniziare la scansione delle sessioni non andate a buon fine.

   Questa opzione è disponibile solo nei sistemi operative Microsoft Windows Vista e successivi.
10. Fare clic su **Avanti**.

    Verrà visualizzata la schermata di configurazione della scansione per poter aggiunger le cartelle da sottoporre a scansione .
11. Fare clic su **Aggiungi Cartella**.
12. Nella finestra Sfoglia cartelle, selezionare le unità e le cartelle da sottoporre a scansione. È possibile aggiungere più unità o cartelle a seconda delle necessità. È inoltre possibile sezionare **Escludi sottocartelle**, per escludere le sottocartelle dalla scansione. Fare clic su **OK**.
13. Nella schermata ‘Configura Pianifica Scansione’, fare clic su **Avanti**.
14. Verificare il riepilogo delle scansioni pianificate.
15. Fare clic su **Fine** per chiudere la finestra di dialogo Pianifica Scansione.
16. Fare clic su **Chiudi** per chiudere la schermata Pianifica Scansione.

Modifica di Pianifica Scansione

Se necessario, è possibile modificare la pianificazione delle scansioni. Per modificare una pianificazione di una scansione, seguire i seguenti passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata delle impostazioni di File & Cartelle.
3. Fare clic su **Pianifica Scansione**.

   Verrà visualizzata la schermata dettagli della scansione pianificata.

4. Selezionare la pianificazione che si desidera modificare e quindi fare clic su **Modifica**.
5. Apportare le modifiche necessarie e quindi fare clic su **Avanti**.
6. Nella schermata 'Configura Pianifica Scansione', è possibile aggiungere o rimuovere le unità e le cartelle a piacimento e quindi fare clic su **Avanti**.
7. Controllare il riepilogo delle modifiche.
8. Fare clic su **Fine** nella finestra di dialogo Pianifica Scansione.
9. Fare clic su **Chiudi** nella schermata Pianifica Scansione.

Eliminare la scansione pianificata

È possibile rimuovere una scansione pianificata in qualsiasi momento. Per rimuovere la scansione pianificata, seguire i seguenti passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Verrà visualizzata la schermata delle impostazioni di File & Cartelle.
3. Fare clic su **Pianifica Scansione**.

   Verrà visualizzata la schermata dettagli della scansione pianificata.
4. Selezionare il piano di scansione che si desidera rimuovere e quindi fare clic su **Rimuovi**.

   Viene visualizzata la schermata di conferma.
5. Fare clic su **SI** per rimuovere la scansione pianificata selezionata.
6. Fare clic su **Chiudi** per chiudere la schermata della scansione pianificata.

Per maggiori informazioni sulla pianificazione delle scansioni, fare riferimento a Impostazioni Scansione.

Esclusioni File & Cartelle

Con Escludi File & Cartelle With Exclude Files & Folders, you can decide which files and folders should not be included during scanning for known viruses or issues, DNA Scan, and packers. This helps you avoid unnecessary repetition of the scanning of files which have already been scanned or that you are sure should not be scanned. You can exclude files from being scanned from the following scanning modules:

Con File & Cartelle, è possibile decidere quali file e cartelle non devono essere inclusi durante la scansione alla ricerca di virus noti o problemi, il DNA Scan e il controllo dei programmi di compressione. Questo consente di evitare inutili ripetizioni della scansione dei file che sono già stati sottoposti a scansione o che si

è sicuri non debbano essere sottoposti a scansione. È possibile escludere i file dalla scansione dai seguenti moduli di scansione:

- Scanner
- Protezione Virus
- Scansione Memoria
- DNAScan

Configurazione Esclusione Files & Cartelle

Per configurare esclusioni File & Cartelle, seguire i seguenti passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Comparirà la finestra impostazioni File & Cartelle.
3. Fare clic su **Escludi File & Cartelle**.

   Viene visualizzata la schermata relativa sotto cui è visibile un elenco di file e cartelle da escludere dalla scansione
4. Per aggingere nuovi file e cartelle, fare clic su **Aggiungi**.

   Viene visualizzata la schermata Escludi nuovi elementi.
5. Nella casella di testo nuovo elemento, fornire il percorso del file o della cartella. È inoltre possibile fare clic sull'icona del file o della cartella per selezionarne il percorso.

   Assicurarsi di aver inserito il percorso corretto, altrimenti verrà visualizzato un messaggio.
6. Sotto 'Escludi da', selezionare i moduli da cui si vuole escludere il controllo del file o della cartella selezionata.

   É possible selezionare il rilevamento di virus noti da DNAScan e file compressi sospetti dalle opzioni di scansione.
7. Fare clic su **OK**.
8. Fare clic su **Salva Modifiche** per salvare le impostazioni.

- Se si riceve un avviso di virus rilevato in un file pulito, è possibile escludere il file dalla scansione.
- Se si riceve un avviso DNAScan in un file pulito, è possible escludere il file dalla scansione DNAScan.

Quarantena & Backup

Con Quarantena & Backup è possibile isolare in modo sicuro i file infetti o sospetti. Quando un file viene aggiunto a Quarantena & Backup, Seqrite Endpoint

Security codifica i file e lo mantiene all'interno della cartella Quarantena. Essendo conservati in forma criptata questi file non possono essere eseguiti, e quindi, sono al sicuro. Quarantena mantiene una copia del file prima di ripararlo se è stato fatto il 'Backup prima della riparazione' dalle impostazioni di scansione.

Con Quarantena & Backup, è possibile configurare le regole di rimozione dei file dopo uno certo periodo di tempo e ottenere un backup dei file.

Configurazione Quarantena & Backup

Per configurare Quarantena & Backup, segui i seguire i seguenti passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **File & Cartelle**.

   Viene visualizzata la schermata di impostazione di File & Cartelle.
3. Fare clic su **Quarantena & Backup**.

   Viene visualizzata la schermata di Quarantena e i dettagli relativi.
4. Selezionare **Elimina file da quarantena/backup dopo** e impostare il numero di giorni dopo i quali eliminare i file. Tuttavia è impostato come predefinito un periodo di 30 giorni.
5. Fare clic su **Visualizza File** per vedere i file in quarantena. Nella lista della quarantena, è possibile eseguire una delle seguenti azioni sui file:
   - Aggiungi: per aggiungere file manualmente alla quarantena da cartelle e unità.
   - Rimuovi: per rimuovere i file in quarantena.
   - Ripristina Selezionato: per ripristinare manualmente i file selezionati se necessario.
   - Rimuovi Tutto: per rimuovere tutti i file in quarantena.
   - Invia: per inviare i file selezionati al nostro laboratorio di ricerca.
   - Chiudi: per chiudere la finestra di dialogo della quarantena.

Email

Con Sicurezza Email, è possibile personalizzare le regole di protezione delle email ricevute. E' possibile impostare regole per bloccare i messaggi email che possono essere sospetti spam o malware.

Sicurezza email include quanto segue.

Protezione Email

Con Protezione Email, è possibile configurare delle regole di protezione per tutte le email in arrivo. È possibile bloccare le email con allegati infetti contenenti spam, virus e sospetti malware. È possibile personalizzare le azioni sulle email nel caso in cui viene rilevato un malware.

Tuttavia, la protezione email è attivata come predefinita e le impostazioni predefinite forniscono la protezione necessaria per la propria mailbox da email nocive. Si consiglia di tenere sempre attiva la protezione email per garantire la protezione della posta elettronica.

Configurare protezione email

Per configurare la protezione email, seguire i seguenti passi:

1. Aprire **Seqrite Endpoint Security**.
2. Nella schermata principale di Seqrite Endpoint Security, fare clic su **Email**.

   Viene visualizzata la schermata delle impostazioni.
3. Abilitare **Protezione Email**.

   Viene attivata la protezione contro i malware provenienti dalle email.

   Comunque, la Protezione Email è abilitata in modo predefinito.
4. Per impostare ulteriori regole di protezione per le email, fare clic su **Protezione Email**.
5. Selezionare **Mostra messaggio di allarme** se si desidera ricevere un messaggio quando viene rilevato un virus nelle email o negli allegati.

   Il messaggio sul virus comprende le seguenti informazioni: nome del virus, indirizzo del mittente, oggetto della email, nome dell' allegato e azione eseguita.
6. In 'Seleziona l'azione da eseguire quando viene rilevato un virus', selezionare **Ripara** per ricevere i messaggi di posta elettronica o allegati riparati quando viene rilevato un virus, o selezionare **Elimina** per eliminare l'email infetta o l'allegato.

   Se l'allegato non può essere riaprato viene eliminato.
7. Selezionare **Backup prima di effettuare azioni** se si vuole eseguire un backup delle email prima di eseguire un'azione su di esse.
8. In 'Controllo impostazioni allegato', selezionare un'opzione per bloccare un certo tipo di email e allegati.
9. Fare clic su **Salva Modifiche** per salvare le impostazioni.

Controllo Impostazioni Allegati

Blocca allegati con estensioni multiple	Consente di bloccare allegati nelle email con estensioni multiple. I Worms utilizzano comunemente estensioni multiple ed è possible bloccarli utilizzando questa opzione.
Blocchi email realizzati per utilizzare le vulnerabilità	Consente di bloccare le email il cui unico scopo è quello di sfruttare le vulnerabilità del client di posta. Messaggi di posta elettronica, come MIME, IFRAME contengono vulnerabilità.
Abilita controllo allegati	Permette di bloccare gli allegati email con estensioni specifiche o tutte le estensioni. Tuttavia, questa opzione non è selezionata come predefinita. Se si vuole selezionare questa opzione, seguire i seguenti modi: **Blocca tutti gli allegati**: per bloccare tutti i tipi di allegati presenti nelle email. **Blocca allegati da specifici utenti:** per bloccare allegati con un determinato tipo di estensione. Se si vuole attivare questa opzione, fare clic su **Configura**: • In 'Estensioni specificate dall'utente', selezionare le estensioni che si vogliono mantenere così da bloccare gli allegati con tali estensioni ed elimnare tutte le estensioni rimanenti. • Se alcune estensioni che si vogliono bloccare non sono presenti nella lista, digitare tali estensioni nella casella di testo delle estensioni e fare clic su **Aggiungi** per aggiungerle alla lista. • Fare clic su **OK** per salvare i cambiamenti.

Protezione Client Email Affidabili

Protezione Client Email Affidabili supporta la maggior parte dei client mail più comuni come Eudora e altri. Se il client email è diverso da quelli proposti nella lista, è possibile aggiungerlo nella lista dei client affidabili.

Configurare Protezione Client Email Affidabili

Per configurare Protezione Client Email Affidabili, seguire questa procedura:

1. Apri **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Email**.

   Si arre la schermata dei dettagli delle impostazioni Email.
3. Attivare la **Protezione Client Email Affidabili**.
4. Per aggiungere un nuovo client email, fare clic su **Protezione Client Email Affidabili**.

   Si apre la schermata dei dettagli di quarta opzione.
5. Fare clic su **Sfoglia** e selezionare un client affidabile
6. Fare clic su **Aggiungi** per aggiungere il client mail alla lista.
7. Fare clic su **Salva Modifiche** per salvare le impostazioni.

Protezione Spam

Con Protezione Spam, è possibile bloccare tutte le email indesiderate come spam, phishing e messaggi con contenuti porno dal raggiungere la propria casella di posta. Protezione Spam è attiva per impostazione predefinita e consigliamo di mantenere sempre questa funzione attiva.

Configurare la Protezione Spam

Per configurare la Protezione Spam, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Email**.

   Si are la schermata dei dettagli delle impostazioni Email.
3. Attivare la **Protezione Spam**.
4. Per impostazioni più approfondite, fare clic su **Protezione Spam**.
5. Selezionare **Tagga oggetto con testo (Raccomandato)**, per etichettare l'oggetto di una mail come SPAM.
6. In **Livello Protezione Spam**, impostare il livello di protezione:
   - Leggero: applica una politica di protezione spam a basso filtraggio.
   - Moderato – assicura un filtraggio ottimale. È raccomandato selezionare il filtraggio moderato, il quale è anche selezionato come impostazione predefinita..
   - Rigoroso – forza un criterio di alto filtraggio ma non è ideale in quanto aumenta la possibilità che anche mail non maligne vengano bloccate. Selezionare questo livello di filtraggio solo quando si ricevono troppe mail spazzatura.
7. Selezionare **Abilita Black List delle email** per applicare i parametri di protezione per le mail nella Black List.
8. Selezionare **Abilita White List delle email** per applicare i parametri di protezione per le mail nella Whitelack List.
9. Selezionare **Abilita plugin AntiSpam** per applicare i parametri di protezione per il plug-in AntiSpam.
10. Fare clic su **Salva Modifiche** per salvare le impostazioni.

Impostare le regole di protezione spam per la Black List

La Black List è una lista di indirizzi mail da cui tutte le mail vengono filtrate a prescindere dal loro contenuto. Tutte le mail provenienti dagli indirizzi nella lista vengono etichettate come "[SPAM] -". Questa funzione deve essere specificatamente evocata nel caso in cui un server abbia un Open Relay che viene utilizzato in modo abusivo da mass mailer e virus.

Per aggiungere indirizzi mail alla Black List, seguire questa procedura:

1. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Abilita Black List Email**.

   Si attiva il tasto Personalizza.

2. Fare clic su **Personalizza**.
3. Inserire un indirizzo mail nella casella di testo della Black List e fare clic su **Aggiungi**.

   Mentre si inserisce un indirizzo mail, fare attenzione a non inserire lo stesso indirizzo mail già inserito nella White List, altrimenti apparirà un messaggio di avviso.

   Per modificare un indirizzo mail, selezionare l'indirizzo mail nella lista e fare clic su **Modifica**. *Per rimuovere un indirizzo mail, selezionare un indirizzo mail e fare clic su* **Rimuovi**.

4. È possibile importare la Black List facendo clic su **Importa Lista**.

   Questa opzione è utile se è stata precedentemente salvata o esportata la lista delle mail.

5. È possibile esportare la Black List cliccando **Esporta Lista**.

   In questo modo si esportano tutti gli indirzzi mail esistenti nella lista. È utile quando si deve reinstallare Seqrite Endpoint Security successivamente o su un altro sistema e si desidera che gli stessi indirizzi mail vengano poi messi in lista.

6. Fare clic su **OK** per salvare le impostazioni.

Impostare le regole di protezione spam per la White List

La White List è una lista di indirizzi mail da cui tutte le mail possono evitare il filtro anti-spam a prescindere dal loro contenuto. Nessuna mail proveniente dagli indirizzi della lista passerà attraverso il filtro SPAM. Suggeriamo di configurare solo quegli indirizzi mail di cui si ha piena fiducia.

Per aggiungere indirizzi mail alla White List, seguire questa procedura:

1. Nella schermata delle impostazioni Protezione Spam, selezionare **Abilita White List Email**.

   Si attiva il tasto Personalizza.

2. Fare clic su **Personalizza**.
3. Inserire un indirizzo mail nella casella di testo della White List e fare clic su **Aggiungi**.

   Mentre si inserisce un indirizzo mail, fare attenzione a non inserire lo stesso indirizzo mail già inserito nella Black List, o apparirà un messaggio di avviso.

   Per modificare un indirizzo mail, selezionare l'indirizzo mail nella lista e fare clic su **Modifica**. *Per rimuovere un indirizzo mail, selezionare un indirizzo mail e fare clic su* **Rimuovi**.

4. È possibile importare la White List cliccando **Importa Lista**.

   Questa opzione è utile se è stata precedentemente salvata o esportata la lista delle mail.

5. È possibile esportare la lista bianca cliccando **Esporta Lista**.

   In questo modo si esportano tutti gli indirzzi mail esistenti nella lista. È utile quando si deve reinstallare Seqrite Endpoint Security successivamente o su un altro sistema e si desidera che gli stessi indirizzi mail vengano poi messi in lista.

6. Fare clic su **OK** per salvare le impostazioni.

Aggiungere domini alla White/Black List

Per aggiungere domini alla White/Black List, seguire questa procedura:

1. Selezionare l'opzione **Abilita White List Email** o **Abilita Black List Email** e poi fare clic su **Personalizza**.
2. Digitare il dominio e fare clic su **Aggiungi**.

   *Il dominio dovrebbe essere in formato: *@mytest.com.*

3. Fare clic su **OK** per salvare i cambiamenti.

Internet & Network

Con Internet & Network, è possibile impostare i parametri di protezione per salvare il sistema da file malevoli che possono infiltarsi nel computer durante le attività di banking online, shopping, navigazione, ecc. È possibile anche impostare il Parental Control per monitorare le attività online dei propri figli e di altri utenti così da impedirgli di accedere a siti web indesiderati.

Internet & Network includono quanto segue.

Protezione Firewall

I parametri del Firewall e altre opzioni ossono essere configurate da remoto attraverso la console QHEPS.

La Protezione Firewall lavora silenziosamente nel background e monitora l'attività della rete per i comportamenti malevoli.. La Protezione Firewall rileva per prima cosa i malware e, se ne trova, li elimina prima che si possano infiltrare nel computer.

Configurare la Protezione Firewall

Per configurare la Protezione Firewall, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Internet & Network**.

Si apre la schermata dei dettagli delle impostazioni di Internet & Network.

3. Attivare la **Protezione Firewall**.

   La Protezione Firewall è attiva.

Protezione Navigazione

Con la Protezione Navigazione, è possibile bloccare i siti malevoli mentre si naviga così da prevenire l'entrata in contatto con siti malevoli. Comunque, la Protezione Navigazione è attiva per impostazione predefinita.

Configurare la Protezione Navigazione

Per configurare la Protezione Navigazione, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Internet & Network**.

   Si apre la schermata dei dettagli delle impostazioni di Internet & Network.

3. Attivare **Protezione Navigazione**.

   La Protezione Navigazione è attiva.

Protezione Malware

Con la Protezione Malware, è possibile proteggere il sistema da minacce come spyware, adware, keylogger, e riskware mentre si è connessi a Internet.

Configurare la Protezione Malware

Per configurare la Protezione Malware, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Internet & Network**.

   Si apre la schermata dei dettagli delle impostazioni di Internet & Network.

3. Attivare la **Protezione Malware**.

   La Protezione Malware è attiva.

Protezione Phishing

Con Protezione Phishing, è possibile prevenire l'accesso a siti di phishing e fraudolenti. Il Phishing è un tentativo fraudolento, di solito attuato via mail, di sottrarre le informazioni personali. Di solito sembra provenire da organizzazioni e siti ben conosciuti, come banche, compagnie e servizi e chiede di visitare il loro sito e di fornire informazioni personali come il numero di carta d credito, o le proprie password.

La Protezione Phishing scansiona in automatico tutte le pagine tutte le pagine web visitate per individuare attività fraudolente proteggendo da qualsiasi attacco di phishing mentre si naviga su Internet. Previene anche il furto di di identità bloccando i siti di phishing così che si possa effettuare lo shopping online, le operazioni bancarie e la navigazione in genere in sicurezza.

Configurare Protezione Phishing

Per configurare la Protezione Phishing, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Internet & Network**.

   Si apre la schermata dei dettagli delle impostazioni di The Internet & Network.
3. Attivare la **Protezione Phishing** .

   La Protezione Phishing è attiva.

Browser Sandbox

Con Browser Sandbox, è possibile applicare un severo meccanismo di sicurezza per prevenire l'accesso a tutti i siti non verificati e non affidabili sia che si tratti di siti commerciali, che di vendita, pubblicità, intrattenimento, e così via.

Configurare Browser Sandbox

Per configurare Browser Sandbox, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Internet & Network**.

   Si apre la schermata dei dettagli delle impostazioni di Internet & Network.
3. Attivare **Browser Sandbox**.
4. Fare clic su **Browser Sandbox**.
4. Selezionare il livello di sicurezza del Browser.

   Tuttavia, l'impostazione predefinita è ideale e ottimale per i nuovi utenti.
5. Fare quanto segue:
   - Per proteggere i dati confidenziali (quali estratti conto bancari, immagini, documenti importanti, ecc) mentre si naviga, selezionare **Previeni il browser dall'accesso a cartelle confidenziali**, e poi selezionare la cartella che si desidera proteggere.

     I dati nella cartella confidenziale non saranno accessibili dal browser e

da altre applicazioni gestite sotto Browser Sandbox, quindi i dati confidenziali saranno al riparo da violazioni.

- Per proteggere i propri dati dal venire manipolati, selezionare **Previeni il browser dal modificare i dati protetti**, e poi selezionare la cartella che si vuole proteggere.

  I dati nella cartella protetta saranno accessibili ma non potranno essere manipolati o modificati.

- Per scaricare un contenuto durante la navigazione in una determinata cartella, selezionare **Consenti al browser di depositare tutti i download nella specifica cartella** e fornire il percorso della cartella.

  Permette di scaricare il contenuto mentre si naviga in una certa cartella di cui si avrà bisogno in futuro.

6. Selezionare **Mostra contorno verde attorno alla finestra del browser** per indicare che il browser è avviato in Sandbox.

   Tuttavia, questa non è una funzione obbligatoria per la sicurezza e quindi se si preferisce è possibile non selezionarla.

7. Per pulire la cache Sandbox, fare clic su il tasto **Elimina**.

   Ciò permette di pulire i file temporanei.

8. Fare clic su **Salva Modifiche** per salvare le te impostazioni.

Avviso News

Con Avviso News, si ricevono nuovi avvisi riguardo news sulla cyber security, importanti informazioni relative a Seqrite, ecc. Le ultime news sono disponibili anche sulla Dashboard di Seqrite. Se non si vogliono ricevere avvisi relativi alle news, disattivare Allerta News.

Disattivare Avviso News

Per disattivare Avviso News, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Internet & Network**.

   Si apre la schermata dei dettagli delle impostazioni di Internet & Network.

3. Disattivare **Allerta News**..

IDS/IPS

Con Prevenzione Intrusioni (IDS/IPS), è possibile boccare attività malevole della rete e i tentativi di sfruttare la vulnerabilità del software.

I parametri IDS/IPS e altre opzioni possono essere configurate da remoto attraverso la console QHEPS.

Configurare IDS/IPS

Per configurare IDS/IPS, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Internet & Network**.

   Si apre la schermata dei dettagli delle impostazioni di Internet & Network.
3. Attivare **IDS/IPS**.

   La protezione per IDS/IPS è attiva.

Drive & Dispositivi esterni

Con Drive & Dispositivi esterni, è possibile impostare i parametri di protezione per tutti i dispositivi e drive esterni come CD, DVD, unità USB, ecc. Quando il sistema entra in contatto con drive e dispositivi esterni, corre il rischio che si possa infiltrare un malware.

Protezione Autorun

La Protezione Autorun protegge il sistema da malware autorun che cercano di infiltrarsi nel tuo sistema attraverso unità USB o CD/DVD usando la funzione autorun del sistema operatvo installato.

Configurare Protezione Autorun

Per configurare la Protezione Autorun, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Drive & Dispositivi esterni**.

   Si apre la schermata dei dettagli delle impostazioni di Drive & Dispositivi esterni.
3. Attivare **Drive & Dispositivi**.

   Protezione Autorun è attiva.

Scansione Drive Esterni

Con Scansione Drives Esterni, è possibile sottoporre a scansione le unità USB nel momento in cui vengono collegate al sistema. Le unità USB dovrebbero essere sempre essere sottoposte a scansione virus prima di accedere al sistema, poichè questi dispositivi sono diventati mezzo di trasferimento rapido di malware da un sistema all'altro.

Configurare Scansione Drive Esterni

Per configurare Scansione Drive Esterni, seguire qusta procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Drive & Dispositivi esterni**.

   Si apre la schermata dei detagli delle impostazioni di Drive & Dispositivi Esterni.
3. Attivare **Scansione Drive Esterni**.

   Scansiona Drive Esterni è attivo.
4. Per maggiori impostazioni, fare clic su **Scansione Drive Esterni**.
5. Selezionare **Scansione solo file sulla root dell'unità**, se si desidera sottoporre a scansione solo i file sulla directory principale dell'unità. I file all'interno delle cartelle vengono saltati. Questa scansione può richiedere poco tempo ma è meno sicura. Tuttavia, questa opzione è selezionata in modo predefinito.
6. Selezionare **Scansione intera unità**, se si desidera sottoporre a scansione tutti i file del dispositivo USB. Questa opzione potrebbe richiedere del tempo ma è più sicura.
7. Fare clic su **Salva Modifiche** per salvare le impostazioni.

Controllo Dispositivi

Con Controllo Dispositivi, gli amministratori possono creare policy con diritti variabili come bloccare l'accesso completo ai dispositivi removibili, permettere la sola lettura e nessun accesso in scrittura così che niente possa essere scritto sui dispositivi esterni, personalizzare l'accesso ai dispositivi. Una volta applicata la policy al gruppo, vengono applicati anche i diritti di accesso.

Le policy per Controllo Dispositivi e altre opzioni possono essere configurate da remoto attraverso la console QHEPS.

Configurare Controllo Dispositivi

Per creare una policy per Controllo Dispositivi, seguire questa procedura:

1. Andare su **Seqrite Endpoint Security > Impostazioni**.
2. Nella schermata delle impostazioni, fare clic su **Controllo Dispositivi**.
3. Per abilitare il Controllo Dispositivi, selezionare **Abilita Controllo Dispositivi**.
4. In **Seleziona policy di accesso per Tipi di Dispositivo**, selezionare una categoria tra le seguenti:
   - Dispositivi di archiviazione
   - Lettori di carte

- Wireless
- Dispositivi Mobili & Portatili
- Interfaccia
- Camera
- Altri

5. Per i dispositivi corrispondenti sotto la relativa categoria, selezionare una delle seguenti voci a seconda delle necessità:
   - Blocca
   - Permetti
   - Sola Lettura

   Nota: le opzioni sotto le categorie sono disponibili solo se la categoria è selezionata.
6. Per salvare le impostazioni, fare clic su **Salva Policy** nella finestra di sinistra.

   La policy viene applicata a tutti i disposiivi configurati nella lista. Se successivamente si aggiunge un dispositivo, anche ad esso verrà applicata la stessa policy personalizzata.

Nota:

Per Client Windows

- Possono essere aggiunte per l'autorizzazione solo Pen Drives USB formattate con NTFS File System.
- Pen Drives USB con GUID Partition Table (GPT) Partition Style non possono essre aggiunte per l'autorizzazione.
- Se un dispositivo autorizzato e criptato viene formattato, verrà trattato come non autorizzato. Quindi, l'Amministratore dovrà aggiungere nuovamente il dispositivo al Controllo Dispositivo e configurare le policy di conseguenza.

Scansione Windows Mobile

Con Scansione Windows Mobile, è possibile applicare le regole per ricevere notifche quando un telefono Windows Mobile che utilizza il cavo USB viene connesso per effettuare una scansione.

Configurare Scansione Windows Mobile

Per configurare Scansione Windows Mobile, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Drive & Dispositivi esterni**.

Si apre la schermata dei dettagli delle impostazioni di Drive & Dispositivi Esterni.

3. Attivare **Scansione Windows Mobile**.

   Scansione Windows Mobile è attivo.

Capitolo 4. La funzione Accesso Rapido

La funzione Accesso Rapido fornisce rapido accesso a importanti funzioni come Scansione, ecc. Fornisce anche le ultime news su Seqrite.

Icona Navigazione Sicura

L'icona Seqrite Endpoint Navigazione Sicura sul desktop permette di avviare il browser predefinito in Sandbox per una navigazione sicura. Ciò permette di navigare in sicurezza anche se Browser Sandbox è stato disattivato.

Scansione

L'opzione Scansione disponibile sulla Dashboard tfornisce varie opzioni per la scansione del sistema in base alle proprie esigenze. È possibile avviare la scansione dell'intero sistema, di singole unità, di unità di rete, USB, di cartelle e file, determinati percorsi e unità, di effettuale la scansione della memoria e la scansione all'avvio. Anche se le impostazioni predefinite per la scansione manuale sono di solito adeguate, è possibile intervenire sulle opzioni per la scansione manuale a piacere.

Effettuare la scansione completa del sistema

Con Scansione Completa del Sistema, è possibile avviare una scansione completa di tutti i file in avvio, unità, cartelle e file sul tuo sistema (escluse le unità di rete mappate).

Per avviare una scansione completa del sistema, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansiona > Scansione Completa del Sistema**.

   Inizia la scansione..

   *Al termine della scansione poi visualizzare il report sotto **Report**.*

Effetuare scansione personalizzata

Con Scansione Personalizzata, è possibile effettuare la scasnione di specifici record, unità, cartelle e file sul sistema a seconda delle proprie necessità. Ciò è utle quando si vogliono sottoporre a scansione solo alcuni elementi e non l'intero sistema.

Per avviare una scansione personalizzata, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansione** > **Scansione personalizzata**.

   Si apre la schermata delle preferenze di scansione.
3. Fare clic su **Aggiungi** e poi inserire il percorso di file e cartelle da sottoporre a scansione. È possibile selezionare più cartelle per la scansione.
4. Dopo aver impostato le preferenze di scansione, fare clic su **Avvia Scansione**.

   Inizia la scansione.

   *Al termine della scansione, è possibile visualizzare il report sotto **Report**.*

Efettuare Scansione della memoria

Per effettuare una scansione della memoria, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansiona** > **Scansiona Memoria**.

   Inizia la scansione.

   *Al termine della scansione, è possibile visualizzare il report sotto **Report**.*

Durante la scansione vengono mostrati i seguenti campi:

File analizzati	Mostra il numero di file sottoposti a scansione.
File archivio / compressi	Mostra il numero di file archivio / compressi sottoposti a scansione.
Minacce rilevate	Mostra il numero di minacce rilevate.
Avvisi DNAScan	Mostra il numero di file rilevati da DNAScan.
Virus Boot/Partition	Mostra il numero di virus rilevati in avvio / nella partizione.
File riparati	Mostra il numero di file malevoli che sono stati riparati.
File in quarantena	Mostra il numero di file malevoli che sono stati messi in quarantena.
File eliminati	Mostra il numero di file malvoli che sono stati eliminati.
I/O errori	Mostra il numero di errori I/O incorsi durante la scansione.
Stato Scansione	Mostra lo stato della scansione in corso.

Eseguire la Scansione all'avvio

Scansione all'avvio è molto utile per ripulire il sistema nel caso in cui il sistema sia gravemente infettato da un virus e non possa essere ripulito poichè tale virus è

attivo. Questo tipo di scansione verrà effettuato al prossimo avvio usando Windows NT Boot Shell.

Per impostare la Scansione all'avvio, seguire questa procedura:

1. Apri **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansiona** > **Boot Time Scan**.

   Scansione all'avvio offre le seguenti opzioni:

   - Scansione veloce: sottopone a scansione solo le locazioni predefinite del sistema che sono ad alto rischio di virus.
   - Scansione dell'intero sistema: effettua la scansione dell'intero sistema e potrebbe richiedere più tempo.

3. Fare clic su **Sì**.
4. Per riavviare il sistema per un'immediata scansione all'avvio, fare clic su **Sì**. Per effettuare la scansione del sistema successivamente, fare clic su **No**.

Eseguire la Scansione Mobile

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansione** > **Scansione Mobile**.
3. Selezionare il dispositivo mobile dalla lista.

   In caso in cui il telefono non sia disponibile nella lista, è necessario aggiungerlo. Per aggiungere il telefono al sistema,vedere la sezione *Scansione Windows Mobile*.

   Inizia la scansione. Al termine della scansione, yè possibile visualizzare il report della scansione sotto ***Report****.*

News

La sezione News mostra gli ultimi aggiornamenti delle informazioni e degli sviluppi provenienti dai laboratori Seqrite. Quando vi ci sono nuove informazioni sulla protezione del computer, allarmi inerenti la sicurezza o altre importanti notizie, le news ad essi relative vengono qui mostrate. Tuttavia, per avere le ultime informazioni, è necessario possedere la versione con licenza del prodotto.

Capitolo 5. Menu Seqrite

Col Menu di Seqrite Endpoint Security, è possibile configurare le impostazioni generali per ricevere gli aggiornamenti in modo automatico, la protezione password di Seqrite Endpoint Security in modo tale che persone non autorizzate non possano cambiare le impostazioni, fornire impostazioni per il supporto proxy e impostare parametri per i report afinchè vengano rimossi dalla lista.

Impostazioni

Con Impostazioni, è possibile applicare vari parametri di protezione come ricevere aggiornamenti da Seqrite al momento del rilascio, la protezione password per le impostazioni, l'impostazione dei parametri per la rimozione dei resoconti e così via. Tuttavia, le impostazioni predefinite sono ottimali e forniscono protezione completa al sistema. Raccomandiamo di cambiare le impostazioni solo quando è strettamente necessario.

Impostazioni include quanto segue.

Aggiornamento Automatico

Con Aggiornamento Automatico, è possibile ricevere gli aggiornamenti in modo automatico per mantenere il software aggiornato con le ultime firme dei virus e proteggere il sistema dai malware più recenti. Seqrite Endpoint Security raccomanda di mantenere sempre attivo Aggiornamento Automatico, che comunque è attivato per impostazione predefinita.

Configurare l'Aggiornamento Automatico

Per configurare l'Aggiornamento Automatico, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

   Vengono mostrati i dettagli delle impostazioni.
3. Attivare **Aggiornamento Automatico**.

   Viene attivato l'Aggiornamento Automatico.
4. Fare clic su **Aggiornamento Automatico**.
5. Selezionare **Mostra finestra notifica aggiornamento**, se si desidera ricevere notifiche sugli aggiornamenti di Seqrite Endpoint Security.

6. Selezionare la modalità di aggiornamento per ricevere gli aggiornamenti da:
   - **Download da Internet** – Permette di scaricare gli aggiornamenti per il sistema da Internet.
   - **Prendi il file di aggiornamento da un pecorso specifico**– Permette di prendere gli aggiornamenti da una cratella locale o da una cartella di rete.
   - **Download dal Server Endpoint Security**– Permette di scaricare gli aggiornamenti per il sistema dal server Seqrite.
7. Per salvare una copia degli aggiornamenti nella cartella locale o in una cartella di rete, selezionare:
   - **Copia il file di aggiornamento in una posizione specifica**
8. Fare clic su **Salva modifiche** per salvare le impostazioni.

Impostazioni Internet

Con Impostazioni Internet, è possibile attivare il supporto proxy, impostare il tipo di proxy, configurare l'indirizzo IP e il portale del proxy per usare la connessione Internet. Se si sta usando un server proxy sulla rete, o Socks Version 4 & 5, è necessario inserire l'indirizzo IP (o il nome del dominio) e il portale del proxy, il server SOCKS V4 & SOCKS V5 nelle impostazioni Internet. Tuttavia, se si configurano le Impostazioni Internet, è necessario inserire username e password.

I seguenti moduli Seqrite richiedono queste modifiche.

- Wizard di Registrazione
- Aggiornamento Rapido
- Messenger

Configurare le Impostazioni Internet

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

   Verrano mostrati i dettagli delle impostazioni.
3. Fare clic su **Impostazioni Internet**.
4. Selezionare **Disabilita Impostazioni proxy**.

   Vengono attivate le finestre di testo del tipo di proxy, server, porta, e credenziali utente.
5. Nell'elenco 'Tipo', selezionare il tipo di proxy da HTTP, SOCKS V4, SOCKS V5 a seconda delle preferenze.
6. Nella finestra di testo 'Server', inserire l'indirizzo IP del server proxy o del dominio.

7. Nella finestra di testo ‘Porta’, inserire il numero di porta del server proxy.

   Il numero di porta è impostato come 80 per HTTP e 1080 per SOCKS V4, SOCKS V5 in base alle impostazioni predefinite.

8. Inserire il proprio nome utente e password.
9. Fare clic su **Salva Modifiche** per salvare le impostazioni.

Ripristino Registro

Il Registro è un database usato per immagazzinare impostazioni e opzioni dei sistemi operativi Microsoft Windows. Contiene informazioni e impostazioni per tutto l’hardware, il software, gli utenti e le preferenze del sistema.

Quando un utente effettua cambiamenti alle impostazioni del Pannello di Controllo, o a Associazioni di File, Policy di Sistema o Installazione nuovi software, i cambiamenti si riflettono e vengono immagazzinati nel Registro. I malware, di solito, hanno come obiettivo il Registro per limitare particolari funzioni del sistema operativo o di altre applicazioni. Possono modificare il registro di sistema in modo che si comporti in modo benefico con il malware al fine di creare poi problemi al sistema.

La funzione Ripristino Registro ripristina l'area critica del registro di sistema e le altre aree colpite dalle modifiche apportate dal malware. Inoltre ripara il Registro di sistema

Configurare il Ripristino Registro

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

   Vengono mostrati i dettagli delle impostazioni.

3. Fare clic su **Ripristino Registro**.
4. Selezionare **Ripristina area critiche del registro di sistema** per ripristinare l’area critica del registro di sistema durante la scansione. Le aree critiche del registro di sistema vengono generalmente modificate dal malware per eseguire automaticamente determinate attività o per evitare l’individuazione o la modifica di determinate applicazioni del sistema come ‘Disabilita Task Manager’ e ‘Disabilita Editor Registro’.
5. Selezionare **Ripara voci malevoli del registro** per effettuare la scansione del registro di sistema relativamente alle voci malevole. Il malware e ciò che ne rimane vengono automaticamente riparati durante la scansione.

Auto Protezione

Con Auto Protezione, è possibile applicare una protezione alla propria applicazione Seqrite Endpoint Security così che i file, cartelle, configurazioni e

voci di registro configurate per la protezione contro i malware non vengano alterati o attaccati in nessun modo.

Configurare Auto Protezione

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

   Viene mostrata la schermata dei dettagli delle impostazioni.
3. Attivare l'**Auto Protezione**.

   Comunque, Auto Protezione è attiva in modo predefinito.

Protezione Password

Con Protezione Password, è possibile restringere l'accesso a Seqrite Endpoint Security così che utenti non autorizzati non possano effettuare cambiamenti nelle impostazioni. Raccomandiamo di mantenere sempre attiva la Protezione Password.

Configurare la Protezione Password

Per configurare la Protezione Password, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

   Viene mostrata la schermata dei dettagli delle impostazioni.
3. Attivare la **Protezione Password**.

   Appare la schermata delle impostazioni Protezione Password.
4. In 'Inserire nuova password', inserire una nuova password se si sta impostando la password per la prima volta, e poi inserire la stessa password in 'Conferma nuova password'.

   Se si sta impostando la password per la prima volta, allora ***Inserisci vecchia password*** *non sarà abilitato.*
5. Fare clic su **Salva Cambiamenti**.

Impostazioni Report

Con Impostazioni Report, è possibile impostare i parametri affinchè i report generati per le varie attività vengano poi rimossi. È possibile specificare il numero dei giorni dopo il quale i report dovrebbero essere rimossi automaticamente dalla lista. È possibile invece mantenere i report in caso di necessità. Tuttavia, l'impostazione predefinita per la cancellazione dei report è di 30 giorni.

Configurare Impostazioni Report

Per configurare le Impostazioni Report, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

   Appare la schermata delle impostazioni Protezione Password.
3. Fare clic su **Protezione Password**.

   Appare la schermata delle Impostazioni Report.
4. Selezionare **Elimina reports dopo**, e poi selezionare il numero di giorni dopo i quali i report dovrebbro venire cancellati automaticamente.

   *Tuttavia, l'impostazione predefinita è 30 giorni. Se si lascia in bianco **Elimina reports dopo**, nessun report verrà rimosso.*
5. Fare clic su **Salva Modifiche** per applicare le impostazioni.

Report Statistiche Virus

Report Statistiche Virus invia il resoconto delle statistiche del rilevamento di virus, generato durante la scansione, al Seqrite Research Center.

Configurare Report Statistiche Virus

Per configurare Report Statistiche Virus, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

   Appare la schermata dei dettagli delle Impostazioni.
3. Attivare **Report Statistiche Virus**.

   Il Report Statistiche Virus viene attivato.

Ripristinare le impostazioni predefinite

Con Ripristina Impostazioni Predefinite, è possibile tornare alle impostazioni predefinite dalle impostazioni personalizzate. È molto utile quando si personalizzano le impostazioni ma non si è più soddisfatti delle impostazioni di sicurezza o si ha qualche dubbio sulla protezione o si crede che la stessa sia compromessa.

Ripristinare le impostazioni predefinite

Per ripristinare le impostazioni predefinite, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Impostazioni**.

Appare la schermata dei dettagli delle Impostazioni.

3. In 'Ripristina Impostazioni Predefinite', fare clic su **Tutto predefinito**.

   Seqrite Endpoint Security torna alle impostazioni predefinite.

Strumenti

Con Strumenti, è possibile compiere diverse azioni, come ripristinare le impostazioni, prevenire l'accesso a determinate unità, effettuare una diagnosi del sistema e così via.

Strumenti include le seguenti opzioni.

Ripristino Hijack

Con Ripristino Hijack, è possibile riportare le impostazioni modificate di Internet Explorer a impostazioni predefinite. Se si sono modificate le impostazioni predefinite di Internet Explorer o se le impostazioni sono state modificate da malware, spyware, oppure da applicazioni non malevole, è possibile ripristinare le impostazioni predefinite di Internet Explorer usando la funzione Hijack Restore. Questa funzione permette anche di ripristinare impostazioni critiche del sistema operativo come Editor Registro e Task Manager.

Usare Ripristino Hijack

Per usare Ripristino Hijack, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.

3. In 'Strumenti di Pulizia e Ripristino', fare clic su **Ripristino Hijack**.

   Appare la schermata di Rispristino Hijack.

4. Fare clic su **Seleziona Tutti** per selezionare tutte le impostazioni browser dela lista.
5. Selezionare **Ripristina il file Host di default**, per ripristinare il file host di default.
6. Selezionare **Ripristina importanti impostazioni di sistema**, per ripristinare le impostazioni di sistema importanti.
7. Per avviare il ripristino delle impostazioni di sistema, fare clic su **Ripristina Ora**.

Ripristina File Host di default

Questa funzione include quanto segue:

Indirizzo IP	Inserirel'indirizzo IP dell'host.
Host Name	Inserire il nome dell' host.
Aggiungi	Fare clic su **Aggiungi** per aggiungere dettagli dell'host alla lista.
Modifica	Selezionare l'host nella lista e fare clic su **Modifica** per effettuare cambiamenti.
Elimina	Selezionare l'host nella lista e fare clic su **Elimina** per rimuovere l' host.
OK	Fare clic su **OK** per salvare le impostazioni per I file host ed uscire dalla finestra Specifiche Host.
Chiudi	Fare clic su **Chiudi** per uscire dalla finestra Specifiche Host senza salvare le impostazioni.

Ripristina importanti impostazioni di sistema

La funzione Ripristina importanti impostazioni di sistema include quanto segue.

Seleziona tutto	Permette di ripristinare tutte le impostazioni di sistema della lista.
OK	Permette di salvare tutte le impostazioni modificate e ad uscire dalla finestra Importanti Impostazioni di Sistema.
Chiudi	Permette di uscire dalla finestra Importanti Impostazioni di Sistema senza salvare le impostazioni.

I pulsanti nella funzione Hijack Restore e le loro caratteristiche:

Ripristina Ora	Permette di avviare il ripristino delle impostazioni che sono state selezionate.
Annulla	Permette di tornare alle Impostazioni predefinite. Facendo clic su Annulla si apre una finestra **Annulla operazioni**. Le impostazioni che sono state ripristinate a impostazioni predefinite vengono messe in lista. Selezionare alcune impostazioni oppure scegliere **Seleziona tutto** per selezionare tutte le impostazioni. Fare clic su **OK** per tornare alle impostazioni esistenti.
Chiudi	Permette di uscre dalla finestra di Ripristino Hijack senza salvare le impostazioni.

Pulizia Tracce

Con Pulizia Tracce, è possibile rimuovere le applicazioni più recenti (MRU) per assicurarsi che non venga violata la privacy. La maggior parte delle applicazioni immagazzina la lista dei file recenti per consentire di riaprirli per un accesso rapido. Tuttavia, nel caso in cui un sistema venga usato da più di un utente, la privacy dell'utente potrebbe essere compromessa. Pulizia Tracce permette di rimuovere le tracce di queste applicazioni e a prevenire una violazione della privacy.

Usare Pulizia Tracce

Per usare Pulizia Tracce, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
3. In Strumenti Pulizia & Ripristino, fare clic su **Pulizia Tracce**.

   Appare la schermata di Pulizia Tracce.
4. Selezionare le applicazioni delle quali si volgiono rimuovere le tracce o fare clic su **Seleziona Tutto** per selezionare tute le applicazioni della lista.
5. Per avviare la pulizia, fare clic su **Avvia Pulizia**.
6. Una volta completato il processo, fare clic su **Chiudi** per uscire.

Anti-Rootkit

Con Anti-Rootkit, è possibile rilevare ed eliminare rootkit attivi nel sistema. Questo programma scansiona elementi come Processi attivi, Registro di Windows e Files e Cartelle per individuare qualsiasi attività sospetta e rileva i rootkits senza firma. Anti-Rootkit rileva la maggior parte dei rootkits esistenti ed è disegnato per rilevare i rootkits in arrivo e anche per fornire l'opzione di eliminazione.

Tuttavia, raccomandiamo che Seqrite Anti-Rootkit venga usato da una persona che abbia una certa conoscenza del sistema operativo o con l'aiuto di un ingegnere del Supporto Tecnico Seqrite. L'utilizzo improprio di questo programma può portare a un'instabilità del sistema.

Usare Anti-Rootkit

Per usare Anti-Rootkit, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
3. In Strumenti Pulizia & Ripristino, fare clic su **Anti-Rootkit**.

   Si apre una pop-up che raccomanda di chiudere tutte le altre applicazioni prima di avviare Anti-Rootkit.
4. Nella finestra di sinistra della schermata di Anti-Rootkit, fare clic su **Inizia Scansione**.

   Seqrite Anti-Rootkit inizia la scansione del sistema per individuare attività sospette da parte di un rootkit nell'avvio di Processi, Registro di Windows e Files e Cartelle.

Dopo il completamento della scansione, viene mostrato il risultato in tre diverse schede,

5. Selezionare l'azione appropriata contro ogni minaccia evidenziata.

   Dopo aver agito, è necessario riavviare il sistema così che abbia luogo l'eliminazione del rootkit.

Interrompi scansione	Permette di fermare la scansione mentre è in atto.
Chiudi	Permette di chiudere l'Anti-Rootkit. Se decidi di chiudere l'Anti-Rootkit mentre sta avendo luogo la scansione, ti verrà suggrto di fermare la scansione.
Invio Report Errori	A causa di un'infezione o di alcune condizioni inaspettate del sistema, la scansione di Seqrite Anti-Rootkit potrebbe fallire. In caso di fallimento, verrà chiesto di effettuare nuovamente la scansione del sistema e di sottoporre il report degli errori al team Seqrite per ulteriori analisi.

Con l'aiuto della funzione Impostazioni nella schermata Anti-Rootkit, è possibile selezionare gli elementi da sottoporre a scansione durante il processo.

Configurare le impostazioni di Anti-Rootkit

1. Aprire **Seqrite Anti-Rootkit**.
2. Nella schermata Seqrite Anti-Rootkit, fare clic su **Strumenti**.

   Appare la finestra di dialogo Strumenti.

3. Seqrite Anti-Rootkit is configured for Auto Scan by default where it scans the required system areas.
4. Seqrite Anti-Rootkit è configurato per la scansione automatica di default in cui analizza le aree di sistema necessarie.

Scansione automatica	La scansione automatica è una impostazione predefinita per Anti-Rootkit. In Scansione Automatica Seqrite Anti-Rootkit scansiona le aree di sistema predefinite, come: • Processi nascosti. • Voci nascoste di Registro. • File e cartelle nascosti. • ADS eseguibili.

Scansione personalizzata	Permette di personalizzare le impostazioni di scansione per Anti-Rootkit per quanto segue: **Rileva Processi Nascosti** – effettua la scansione di processi nascosti nel sistema. **Rileva elementi nascosti del Registro** – effettua la scansione di elementi nascosti nel Registro di Windows.

	Rileva File e Cartelle nascosti – effettua la scansione di file e

	cartelle nascosti presenti nel sistema e ADS (Alternate Data Streams) eseguibili. È possibile scegliere: • Analizza l'unità sulla quale è installato il sistema operativo • Analizza tutti i drive • ADS (Alternate Data Streams) per effettuare la scansione di ADS eseguibili.
Percorso File Report	Seqrite Anti-Rootkit crea un file report della scansione e lo colloca dove viene eseguito. Tuttavia, è possibile specificare una collocazione diversa.

Visione d'insieme degli Alternate Data Streams – ADS

L'ADS, permette che i dati vengano immagazzinati in file nascosti che sono collegati a file normalmente visibili. Gli Streams non hanno limite di grandezza e ci può essere più di uno stream collegato a un file normale. La ragione primaria per cui un ADS rappresenta un rischio per la sicurezza è che essi sono quasi completamente nascosti e rapresentano forse la cosa più vicina a un nascondiglio perfetto su un file system – situazione ideale per la quale i Trojan possono trarre vantaggio. Gli ADS possono essere facilmente creati/scritti/letti, permettendo a agli autori di Trojan o virus trarre vantaggio da un'area file nascosta.

Risultati Scansione e Pulizia Rootkits

1. Aprire **Seqrite Anti-Rootkit**.
2. Nella finestra a sinistra della schermata di Seqrite Anti-Rootkit, fare clic su **Avvia Scansione**.
3. Seqrite Anti-Rootkit inizia ail tuod effettuare la scansione del sistema alla ricerca di attività sospetta di rootkit in processi in atto, Registro di Windows e File e Cartelle.

   Al termine della scansione, viene mostrato il risultato in tre diverse schede.

   Per agire in modo appropriato è necessario riavviare il sistema di modo che abbia luogo la pulizia del rootkit.

Azioni da intraprendere su Risultati Scansione

Processo	Al termine della scansione, Seqrite Anti-Rootkit rileverà e mostrerà una lista di Processi nascosti. È possibile selezionare i processi da terminare ma assicurarsi che la lista dei processi da terminare non includa processi conosciuti come affidabili. Seqrite Anti-Rootkit mostra anche un riepilogo del processo di scansione a proposito del numero di processi sottoposti a scansione e del numero di processi nascosti rilevati.
Termina processi nascosti	Dopo aver selezionato la lista dei processi da terminare, fare clic su Termina. Se un processo viene terminato con successo, il suo campo PID (Process Identifier) mostrerà il n/a e al nome del processo verrà aggiunta la voce Termonato. Tutti i processi terminati verranno rinominati dopo il riavvio.

Registro	Simile alla scansione Processi, Seqrite Anti-Rootkit mostra una lista delle chiavi di registro nascoste. È possibile selezionare le chiavi per rinominarle ma assicurarsi che una lista delle chiavi da rinominare non includa alcuna chiave di registro conosciuta come affidabile. Seqrite Anti-Rootkit mostra anche un riepiologo del Registro Scansioni sul numero totale di elementi sottoposti a scansione e sul numero degli elementi nascosti rilevati.
Rinominare chiavi di registro nascoste	Dopo aver selezionato una lista di chiavi da rinominare, fare clic su Rinomina. L'operazione richiede il riavvio perciò il Nome chiave sarà preceduto da Rinomina in coda.

File e Cartelle	In modo similare, Seqrite Anti-Rootkit mostra una lista di File e delle Cartelle nascosti. È possibile selezionare File e Cartelle per rinominarli ma assicurrsi che la lista di File e Cartelle da rinominare non incuda alcun file conosciuto come affidabile. Seqrite Anti-Rootkit mostra anche una lista dei Alternate Data Streams eseguibili. Seqrite Anti-Rootkit mostra infine un riepilogo dei file analizzati sul numero totale dei file sottoposti a scansione e sul numero di file nascosti rilevati.
Rinomina file e Cartelle nascosti	Dopo aver selezionato una lista di File e Cartelle da rinominare, fare clic su Rinomina. L'operazione richiede il riavvio perciò il nome di File e Cartelle sarà preceduto da Rinomina in coda.

Eliminare Rootkit attraverso Seqrite Emergency Disk

Alcune volte, i rootkit non vengono eliminati e riappaiono durante la scansione di Seqrite Anti-Rootkit. In questo caso, è possibile anche usare il Seqrite Emergency Disk per una pulizia adeguata. Per effettuare una pulizia in questo modo, creare il Seqrite Emergency Disk e avviarre il sistema attraverso di esso.

Per creare il Seqrite Emergency Disk e usarlo per pulire il sistema, seguire questa procedura:

Passo 1

Per creare Seqrite Emergency Disk, seguire le indicazioni presenti qui: Crea Emergency Disk.

Passo 2

1. Aprire **Seqrite Anti-Rootkit**.
2. Nella finestra di snistra della schermata di Seqrite Anti-Rootkit, fare clic su **Avvia Scansione**.

   Seqrite Anti-Rootkit avvia la scansione del sistema per sospetta attività da parte di rootkit in Processi in corso, Registro di Windows e File e Cartelle.

   Al termine, apparirà il risultato della scansione in tre diverse schede.

3. Agire in modo appropriato contro ogni minaccia evidenziata. Per esempio, è possibile terminare il processo di un rootkit o rinominare il registro delle voci o file di rootkit.

Passo 3

1. Avviare il sistema usando il **Seqrite Emergency Disk**.
2. Il Seqrite Emergency Disk effettuerà automaticamente la scansione del sistema ed eliminerà i rootkit.

Creare l'Emergency Disk

È possibile creare il proprio Emergency Disk di avvio che permetterà di avviare il proprio sistema Windows e sottoporre a scansione tutte le unità, incluse le componenti di NTFS. L'Emergency Disk permette di ripulire i sistemi infettati da virus che colpiscono file che non possono essere eliminati all'interno di Windows.

L'Emergency Disk verrà creato con la definizione delle ultime firme dei virus usata da Seqrite Endpoint Security sul proprio sistema.

Per creare un Emergency Disk, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
3. In 'Strumenti di Pulizia & Ripristino', fare clic su **Crea Emergency Disk**.
4. Nella schermata 'Crea Emergency Disk', fare clic sul link e scaricare il pacchetto necessario.
5. Estrarre il pacchetto scaricato nel proprio sistema. Per esempio, c:\my documents\qhemgpkg.
6. Fornire il percorso del pacchetto e fare clic su **Avanti**.
7. Per creare l'Emergency Disk, selezionare una delle opzioni che vengono mostrate nella schermata. Per esempio, selezionare **Crea Emergency USB Disk** o **Crea Emergency CD/DVD**.
8. Selezionare l'unità disco da convertire in Emergency Disk e fare clic su **Avanti**.

   Appare un messaggio di conferma quando la creazione dell'Emergency Disk ha avuto successo.

Cosa ricordare durante la creazione di un Emergency Disk

- É raccomandabile tenere una copia del pacchetto estratto sul proprio sistema.
- Su sistemi operativi XP e Windows 2003, è necessario prima installare **Imaging API versione 2.0 patch**.

- Quando si usano dispositivi USB, CD/DVD riscrivibili, fare un backup, poichè il dispositivo verrà formattato.
- Per avviare il sistema con USB o CD/DVD, è necessario impostare la sequenza di avvio in BIOS.
- Una volta terminata la scansione, si deve rimuovere l'Emergency USB disk o CD/DVD prima di riavviare il computer altrimenti il sistema sarà di nuovo avviato partendo dal Emergency Disk

Usare l'Emergency Disk

1. Inserire l'**Emergency Disk** nel drive CD/DVD/USB.
2. Riavviare il sistema.
3. L'Emergency Disk avvia la scansione di tutti i drive in modo automatico. Pulirà da infezioni, se ne vengono rilevate.
4. Riavviare il sistema.

Avvio AntiMalware

Seqrite AntiMalware, col suo meccanismo di scansione malware migliorato, effettua la scansione di registro, file e cartelle ad alta velocità per rilevare ed eliminare Spyware, Adware, Rogueware, Dialer, Riskware e molte altre potenziali minacce nel sistema.

Avviare Seqrite AntiMalware

Seqrite AntiMalware può essere avviato in uno dei seguenti modi:

1. Selezionare **Start > Programmi > Seqrite Endpoint Security > Seqrite AntiMalware**.
2. Fare click destro sull'icona Virus Protection nel barra di sistema di Windows e selezionare **Avvia AntiMalware**.
3. Fare clic su **Strumenti > Avvia AntiMalware** dalla Dashboard Seqrite Endpoint Security.

Usare AntiMalware

Nella schemata di Seqrite AntiMalware, fare clic su **Effettua la scansione ora** per avviare il processo di scansione malware. Mentre avviene la scansione dei malware, Seqrite AntiMalware mostra file malevoli, cartelle ed voci di registro relative a vari malware. Una volta completata la scansione e, in caso sia stato trovato un malware, verrà mostrata una lista dei malware rilevati al'interno di file, cartelle e registri.

È possibile ripulire file, cartelle e registri specifici all'interno della lista, ma prima assicurarsi che tutti gli elementi puliti siano applicazioni autentiche e non malevole.

Nel caso in cui venga trovato un malware, è possibile agire nei seguenti modi:

Pulisci	Permette di eliminare i malware e ciò che ne rimane dal sistema. Se si puliscono file, cartelle o voci di registro specifici, consigliamo di escludere quegli elementi in futuro. Se si desidera escluderli in modo permanente, fare clic su **Sì**, oppure **No** per una esclusione temporanea.
Salta	Permette di saltare l'esecuzione di una qualsiasi azione contro malware presente nel sistema.
Interrompi Scansione	Permette di interrompere la scansione.
Imposta il punto di Ripristino del sistema prima della pulizia	Permette di creare un punto di ripristino del sistema prima che il processo di pulizia inizi. Ciò aiuta a tornare allo stato precedente alla pulizia effettuata da Seqrite AntiMalware usando la funzione Windows Rispristino Sistema. La funzione **Imposta il punto di rispristino prima della pulizia** non è disponibile su sistemi operativi Windows 2000.
Dettagli	Reindirizza al sito Seqrite.

Visualizza File in Quarantena

Con Quarantena, è possibile isolare i file infetti e sospetti. Quando un file viene aggiunto a Quarantena, Seqrite Endpoint Security cripta il file e lo tiene all'interno dell'archivio Quarantena. Venendo mantenuti sotto forma crittografata, questi file non possono essere eseguiti quindi sono sicuri. La Quarantena mantiene anche una copia del file infetto prima della riparazione. Tuttavia, è possibile effettuare un backup prima di effettuare qualsiasi azione.

Avviare File di Quarantena

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
3. In 'Strumenti di Pulizia & Ripristino', fare clic su **Visualizza Quarantena**.

   Appare una lista dei file in quarantena.

Con Quarantena è possibile effettuare le seguenti azioni:

Aggiungi	Permette did aggiungere file a Quarantena manualmente.
Rimuovi	Permette di rimuovere i file in quarantena.
Ripristina	Permette di ripristinare un file da Quarantena alla sua collocazione originale.
Rimuovi Tutto	Permette di rimuovere tutti i file in quarantena.
Invia	Permette di inviare i file in quarantena ai nostri laboratori di ricerca per analisi maggiori. Selezionare il file da sottoporre e fare clic su **Invia**.

Quando si invia un file in quarantena ai nostri laboratori di ricerca, suggeriamo di fornire il proprio indirizzo mail e la ragione per cui si sottopone il file. Le ragioni possono essere:

File Sospetto	Selezionare questa ragione se si crede che un file in particolare sia la causa di attività sospetta nel sistema.

File irreparabile	Selezionare questa ragione se Seqrite è stato capace di rilevare il file malevolo nel sistema durante la scansione, ma non è stato capace di riparare l'infezione del file.
Falso positivo	Selezionare questa ragione se un file, non malevolo, che si stava usando e della cui funzione si è consapevoli, è stato classificato come file malevolo da Seqrite.

Protezione Unità USB

Con Seqrite Endpoint Security, è possibile salvaguardare i dispositivi USB da malware autorun. La funzione Autorun delle unità removibili è uno dei mezzi con cui i malware si infiltrano nel sistema. La funzione di protezione drive USB previene i malware autorun da utilizzare il dispositivo removibile come mezzo di diffusione per l'infezione. Mettere in sicurezza il dispositivo removibile, assicura che il dispositivo, se connesso ad un sistema infetto, non possa essere usato per diffondere un malware autorun in un altro sistema.

Per salvaguardare dispositivi mobili, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
3. Sotto Strumenti Preventivi, fare clic su **Protezione Unità USB**.
4. Nella lista 'Seleziona un'unità removibile', vengono elencati tutte le unità removibili collegate al sistema. Selezionare l'unità e fare clic su **Metti in sicurezza l'Unità Removibile**.

   Il drive verrà messo in sicurezzao contro malware Autorun quando viene usato in altri sistemi.

   Seqrite raccomanda ti tenere disattivata la funzione Autorun del proprio drive USB, tuttavia, è possibile attivare la funzione Autorun del drive USB seguendo lo stesso processo qui menzionato.

Esplora Sistema

Questo strumento fornisce tutte le informazioni importanti relative al computer, come processi in corso, BHO installati, barre degli strumenti installate in Internet Explorer, ActiveX installati, Hosts, LSPs, Programmi di avvio, impostazioni Internet Explorer e connessioni di rete attive. Ciò permette di effettuare una diagnosi del sistema per tracciare l'esistenza di nuovi malware o riskware.

Per usare Esplora Sistema, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
3. In Strumenti di Diagnostica, fare clic su **System Explorer**.

Windows Spy

Con Windows Spy, è possibile scoprire più informazioni a proposito di un'applicazione o di un processo, quando necessario. A volte, continuiamo a ricevere caselle di dialogo o messaggi che in realtà ci vengono mostrati come spyware o malware e non possiamo localizzare il malware. In questi casi, lo strumento può essere usato per scoprire più informazioni sull'applicazione trascinando un bersaglio sulla finestra che appare sullo schermo. Questo strumento fornisce le seguenti informazioni:

- Nome applicazione
- Nome originale del file
- Nome del produttore
- Descrizione del file
- Versione del file
- Nome interno
- Nome prodotto
- Versione del prodotto
- Informazioni sul Copyright
- Commenti

Usare Windows Spy

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
3. Sotto Strumenti di Diagnostica, fare clic su **Windows Spy**.
4. Trascinare il puntatore del mouse sull'applicazione.

   Si aprirà una fnestra riportante le informazioni sopra citate.
5. Se si desidera terminare l'applicazione o chiudere la finestra, fare clic su **Chiudi Processo**.

Escludi Estensioni File

Con Escludi Estensioni File, è possibile creare una lista di esclusione di tipi di file o estensioni di file dalla Protezione Virus. Ciò aiuta a concentrarsi solo su quei file che sono inclini a un comportamento malevolo.

Creare una Lista di Esclusione per la Virus Protection

6. Aprire **Seqrite Endpoint Security**.
7. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Strumenti**.

   Appare la schermata dei dettagli degli Strumenti.
8. Sotto Strumenti di Diagnostica, fare clic su **Escludi Estensioni di File**.
9. Inserire l'estensione di file che deve essere esclusa dalla scansione di Protezione Virus e fare clic su **Aggiungi**.
10. Se l'estensione aggiunta non è corretta, selezionare l'estensione aggiunta nella lista e fare clic su **Rimuovi** per cancellarla.
11. Fare clic su **OK** per salvare la lista.

Report

Seqrite Endpoint Security crea e mantiene un report dettagliato di tutte le attività importanti come la scansione virus, dettagli degli aggiornamenti, cambiamenti nelle impostazioni delle funzioni, ecc.

Può essere visualizzato un report per ciascuna delle seguenti funzioni di Seqrite Endpoint Security:

- Scanner
- Protezione Virus
- Protezione Email
- Pianificazione Scansioni
- Aggiornamento Rapido
- Scansione Memoria
- Protezione Phishing
- Ripristino Registro
- Scansione all'avvio
- Scansione AntiMalware
- Protezione Firewall
- Web Security
- IDS & IPS
- Protezione Navigazione
- Scansione PC2Mobile

Visualizza Report

Per visualizzare i report e le statistiche delle diferenti funzioni, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, fare clic su **Report**.

   Appare la lista dei Report..
3. Nella lista **Report per**, fare clic sulla funzione per la quale si desidera visualizzare il report.

Appare la lista dei dettagli del report sulla finestra a destra. Le statistiche del report per qualsiasi funzione includono Data e Ora della creazione del report e la ragione per cui è stato creato.

Pulsante	Azione
Dettagli	Permette di visualizzare un report dettagliato del record selezionato nella lista.
Elimina Tutto	Permette di eliminare tutti i record nella lista.
Elimina	Permette di eliminare i record selezionati nella lista.
Chiudi	Permette di chiudere la schermata dei report.

È possibile visualizzare maggiori dettagli su un report di una funzione. Nella finestra di destra, fare clic sul report per visualizzare i dettagli. Si apre la schermata con i dettagli del report, che include quanto segue:

Tasto	Azione
Precedente	Permette di visualizzare il report dettagliato dei record precedenti della lista. Questo pulsante non è attivo se il record selezionato è il primo della lista.
Successivo	Permette di visualizzare il report dettagliato del record successivo nella lista. Questo pulsante non è attivo se il record selezionato è l'ultimo della lista.
Stampa	Permette di fare una stampa del report dettagliato.
Salva come	Permette di salvare il report dettagliato in formato .txt all'interno del sistema.
Chiudi	Permette di uscire dalla schermata dei dettagli dei report.

Per maggiori dettagli sui Report, vedere Report.

Aiuto

Con la funzione Aiuto, è possibile accedere ai temi di Aiuto quando preferisci, per capire come usare e configurare le funzioni di Seqrite Endpoint Security, come cercare supporto da Quick Heal Technologies Pvt. Ltd., come aggiornare il prodotto, e vedere una lista dei dettagli di licenza del prodotto.

Con la funzione Guida, è possibile accedere agli argomenti della Guida ogni volta che si desiderano informazioni su come utilizzare e configurare le funzionalità di Seqrite Endpoint Security, come ottenere il supporto di Quick Heal Technologies Pvt. Ltd., come aggiornare il prodotto e infine vedere i dettagli della licenza del prodotto.

La funzione Guida comprende i seguenti argomenti.

- **Guida**: consente di selezionare gli argomenti della Guida a prescindere se si è connessi a Internet o no. Selezionando **Aiuto > Guida**, si viene reindirizzati

alla pagina Aiuto dove è possibile trovare argomenti che descrivono le funzioni del prodotto e come usarle. (In alternativa, premere **F1**, o fare clic su **Aiuto** in una finestra dialogo per entrare nella pagina Guida).

- **Invio Informazioni di Sistema**: Permette di inviare informazioni sul proprio sistema a Seqrite per le analisi.

  Per ulteriori dettagli su come inviare le Informazioni di Sistema, vedere Informazioni di Sistema.

- **Supporto**: Permette di richiedere supporto dal Customer Care di Quick Heal Technologies Pvt. Ltd. ogni volta che si incontrano problemi riguardanti il prodotto o le sue funzioni. Il Supporto offre le seguenti opzioni: SupportoWeb (Consultare le FAQ), Supporto Email, Supporto Telefonico, e Supporto Live Chat. È possibile anche inviare le informazioni di sistema e chiedere ai responsabili tecnici di Seqrite di accedere al proprio sistema da remoto per risolvere un probema.

  Per ulteriori dettagli sul Supporto, vedere Supporto.

- **Informazioni su**: la sezione Informazioni su Seqrite Endpoint Security include:
  - Versione di Seqrite Endpoint Security
  - Dettagli della Licenza
  - Validità della Licenza
  - Opzione Aggiorna Ora

Nella sezione Informazioni su, sono disponibili anche i seguenti pulsanti:

Rinnova Ora	Permette di rinnovare la tua iscrizione attuale.
Dettagli Licenza	Permette di accedere alle informazioni sulla Licenza ed al Contratto di Licenza con l'Utente finale (EULA). **Aggiorna Dettagli Licenza**: Questa funzione è utile per sincronizzare le informazioni di Licenza Attuale col Server di attivazione Seqrite. Se si desidera rinnovare la propria licenza e non si sa come farlo o si riscontra un problema durante il rinnovo, è possibile chiamare il team di Supporto Seqrite, fornire la chiave del proprio prodotto e il Codice di Rinnovo. Il team di Supporto Seqrite rinnoverà la licenza. Tuttavia, si deve seguire questa procedura: 1. Connettersi a Internet. 2. Fare clic su **Dettagli di Aggiornamento Licenza**. 3. Fare clic su **Continua** per aggiornare la propria licenza. **Stampa Dettagli Licenza**: Fare clic su Stampa Dettagli Licenza per avere una stampa con le informazioni relativa alla propria iscrizione attuale.
Aggiorna Ora	Permette di aggiornare il database dei virus di Seqrite Endpoint Security.

Informazioni di Sistema

Informazioni di Sistema è uno strumento essenziale per raccogliere informazioni fondamentali di un sistema Windows nei seguenti casi:

Rileva nuovi Malware	Questro strumento raccoglie informazioni per rilevare nuovi Malware da processi in corso, Registro, fle di sistema come Config.Sys, Autoexec.bat ecc.
Ottieni informazioni su Seqrite Endpoint Security	Raccoglie nformazioni sulla versione installata di Seqrite Endpoint Security, le impostazioni di configurazione e i file in Quarantena.

Invio file informazioni di sistema

Questo strumento genera un file INFO.QHC in C:\ e lo invia a Seqrite automaticamente.

Il file INFO.QHC contiene dettagli fondamentali sul sistema e dettagli sulla versione di Seqrite Endpoint Security installata sul sistema in formato binario e di testo. L’informazione contiene l’esecuzione automatica di file (attraverso Registro, Autoexec.bat, System.ini e Win.ini) e processi in atto con i dettagli delle loro librerie supportate. Questi dettagli vengono usati per analizzare il sistema per nuovi Malware e funzionalità proprie di Seqrite Endpoint Security. Le informazioni sopra riportate forniscono servizi migliori e più adeguati ai clienti. Questro strumento non raccoglie altre informazioni personali identificabili, come password, nè condividiamo o riveliamo queste informazioni con nessuno. Noi rispettiamo la vostra privacy.

Generare Informazioni di Sistema

Per generare informazioni di sistema, seguire questa procedura:

1. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Aiuto > Sottoponi Informazioni di Sistema**.

   Si apre il wizard delle Informazioni d Sistema.
2. Fare clic su **Avanti** per continuare.
3. Selezionare una ragione per cui si inviano le informazioni di sistema. Se si sospetta che ci sia un nuovo Malware nel sistema, selezionare **Sospetto che il sistema sia infetto da un nuovo Malware** o se si stanno riscontrando problemi durante l’utilizzo di Seqrite Endpoint Security, selezionare **Sto avendo problemi durante l’utilizzo di Seqrite**. Aggiungere commenti nella casella dei **Commenti** e inserire il proprio indirizzo mail.
4. Fare clic su **Fine**.
5. Veranno generate informazioni di sistema (INFO.QHC) e saranno inviate al Supporto Tecnico di Seqrite.

Capitolo 6.

Usare PC2Mobiles Scan

La funzione Seqrite PC2Mobile Scan è disponibile in Seqrite Endpoint Security. Questa funzione effettua la scansione del telefono alla ricerca di virus, spyware e altri malware. Per sottoporre a scansione il proprio dispositivo mobile, è necessario connetterlo al PC usando uno di questi metodi:

- Cavo USB
- Bluetooth

Continuiamo regolarmente ad aggiungere supporto per i nuovi modelli. Per la lista più recente dei modelli supportati, vedere www.quickheal.co.in/pc2mobile.asp.

Requisiti importanti per PC2Mobile Scan

- Questa funzione è supportata solo su sistemi operativi Microsoft Windows XP, Windows Vista e Windows 7.
- Per i dispositivi Windows Mobile, è necessario avere installato sul PC Microsoft Active Sync 4.5, o versioni successive ad essa.
- Per i cellulari Nokia, è raccomandabile installare il software Nokia PC Suite sul sistema del computer. Per tutti gli altri dispositivi mobili, è raccomandabile aver installato sul sistema i driver relativi.
- Per la connessione Bluetooth, il sistema dovrebbe avere un dispositivo Bluetooth con driver installati in modo appropriato.
- Sono supportati solo drive Microsoft, Broadcom e Widcomm per i dispositivi Bluetooth. Per ottenere risultati migliori, raccomandiamo di installare i drive Microsoft per i dispositivi Bluetooth.
- Per la connessione Bluetooth tra dispositivi mobili e PC, alcuni modelli di telefoni devono installare il Connector Seqrite. Il wizard di Seqrite Mobile connection Permette di installare Seqrite Connector sul proprio dispositivo mobile.

Configurare Windows Mobile Phone prima della Scansione

Per configurare un telefono Windows Mobile, seguire questa procedura:

1. Connettere il proprio SmartPhone Windows al PC o al Laptop attraverso il cavo USB.

   *Per Windows XP, assicurarsi che **Microsoft Active Sync 4.5** o versioni successive sia installato e venga avviato. Per Windows Vista e Windows 7, che sia installato e avviato **Windows Mobile Device Center**.*

2. Avviare **Seqrite Endpoint Security**.
3. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansione > Scansione Mobile**.
4. Nel Wizard 'Scansione Mobile', fare clic su **Aggiungi Telefono**.
5. Selezionare **Windows Mobile** e fare clic su **Avanti**.

   Il Wizard di Endpoint Security Mobile Connection cercherà dispositivi Windows Mobile collegati al tuo computer.

6. Dopo che la ricerca del Windows Mobile è andata a buon fine, fare clic su **Termina** per competare la configurazione del telefono.

   Una volta configurato con successo, il Windows Mobile viene aggiunto all'elenco dei Dispositivi.

Scansione di Windows Mobile

Per sottoporre a scansione un Windows Mobile, seguire questa procedura:

1. Avviare **Seqrite Endpoint Security**.
2. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansione > Scansione Dispositivo**.
3. Selezionare il dispositivo mobile dall'elenco.
4. Fare clic su **Scansione** per avviare la scansione.

Notifiche di Scansione per Windows Mobile quando è connesso al PC

Quando si connette il Windows Mobile al PC usando un cavo USB, Seqrite Endpoint Security PC2Mobile lo rileva e suggerisce di effettuare la scansione.

Configurare altri dispositivi mobili prima della scansione

Altri dispositivi mobili possono essere configurati sul sistema nei seguenti modi.

Connessione attraverso Bluetooth

Per configurare un dispositivo mobile via Bluetooth, seguire questa procedra:

1. Connettere il dispositivo mobile al PC o Laptop attraverso Bluetooth.

   Assicurarsi di essere abilitaio a connettere il dispositivo mobile al sistema via Bluetooth.
2. Avviare **Seqrite Endpoint Security**.
3. Sulla Dashboard Seqrite Endpoint Security, selezionare **Scansione** > **Scansione Mobile**.
4. Nel Wizard di Scansione Mobile, fare clic su **Aggiungi Dispositivo**.
5. Selezionare **Altri dispositivi mobili**.
6. Selezionare il dispositivo mobile dalla lista dei dispositivi mobili e fare clic su **Avanti**.

   Il Wizard della Mobile Connection cerca il telefono e mostra le connessioni Bluetooth disponibili per il computer.
7. Selezionare il dspositivo mobile dalla lista dei dispositivi mobili e fare clic su **Avanti**.
8. Se il telefono ha bisogno del Seqrite Connector installato, seguire questa procedura per installare Seqrite Connector sul dispositivo mobile.

   i. Fare clic su **Installa Connector**.

      *Il wizard Endpoint Security Mobile Connection invierà l'installer di **Seqrite Connector** al telefono.*

      Si riceverà un messaggio sul telefono. Seguire le indicazioni del messaggio per installare Seqrite Connector sul telefono.

   ii. Dopo la installazione selezionare **Avvia Seqrite Connector** dal telefono.

   iii. Fare clic su **Avanti**.
9. Fare clic su **Termina** per completare la configurazione.

   Una volta che il Bluetooth Mobile è configurato con successo, viene aggiunto alla lista Seqrite Endpoint Security Mobile.

Scansione di altri dispositivi mobili attraverso Bluetooth.

Per sottoporre a scansione altri dispositivi mobili via Bluetooth, seguire questa procedura:

1. Connettere il telefono al PC o Laptop attraverso il Bluetooth.

   Assicurarsi di essere abilitati a connettere il dispositivo mobile al sistema via Bluetooth.

2. Avviare **Seqrite Endpoint Security**.
3. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansione** > **Scansione Mobile**.
4. Selezionare il telefono dalla lista.
5. Fare clic su **Scansione** per avviare la scansione.

Connessione attraverso cavo USB

Per configurare il telefono via cavo USB, seguire questa procedura:

1. Connettere il telefono al PC o Laptop attraverso il cavo.

   Assicurarsi di essere abilitati a connettere il dispositivo mobile al PC via cavo.

2. Avviare **Seqrite Endpoint Security**.
3. Sulla Dashboard di Seqrite Endpoint Security, selezionare selezionare **Scansione** > **Scansione Mobile**.
4. Fare clic su **Aggiungi Telefono**.
5. Selezionare **Altro dispositivo Mobile**.
6. Selezionare il telefono dalla lista e fare clic su **Avanti**.
7. Fare clic su **Termina** per completare la configurazine del telefono.

   Una volta ache il Cavo è configurato con sucesso, viene aggiunto alla lista dei telefoni.

Scansione di altri dispositivi mobili attraverso il cavo USB.

Per sottoporre a scansione altri dispositivi mobili via cavo USB, seguire questa procedura:

1. Connettere il telefono al PC o Laptop attraverso il cavo USB.

   Assicurarsi di essere abilitati a connettere il dispositivo mobile al PC via cavo.

2. Avviare **Seqrite Endpoint Security**.
3. Sulla Dashboard di Seqrite Endpoint Security, selezionare **Scansione** > **Scansione Mobile**.

4. Selezionare il telefono dalla lista.
5. Fare clic su **Scansione** per avviare la scansione.

Capitolo 7. Aggiornanmento di Seqrite Endpoint Security & Pulizia Virus

Gli aggionamenti per Seqrite Endpoint Security vengono rilasciati regolarmente sul sito di Seqrite, il quale contiene informazioni pertinenti ala scoperta e alla rimozione dei virus trovati. Per proteggere il tuo sistema da nuovi virus, è necessario avere una copia sempre aggiornata di Seqrite Endpoint Security. L'impostazione predefinita di Seqrite Endpoint Security è configurata in modo da raccogliere gli aggiornamenti in modo automatico, senza l'intervento dell'utente.

Alcune precisazioni importanti sugli aggiornamenti di Seqrite Endpoint Security:

- Tutti gli aggiornamenti di Seqrite Endpoint Security sono aggiornamenti completi che includono l'aggiornamento del file delle definizioni dei virus e l'aggiornamento del motore di scansione.
- Tutti gli aggiornamenti Seqrite Endpoint Security attualizzano la propria versione quando necessario, fornendo perciò man mano le nuove funzioni e la nuova tecnologia finalizzata alla massima protezione.
- Seqrite Endpoint Security Update è un processo di aggiornamento che si effettua in un unico passaggio.

Aggiornare Seqrite Endpoint Security da Internet

Con Aggiorna Adesso, è possibile aggiornare Seqrite Endpoint Security manualmente e quando si preferisce. Tuttavia, l'impostazione predefinita di Seqrite Endpoint Security è configurata per ricevere gli aggiornamenti in automatico tramite Internet. Il sistema deve essere connesso a Internet per ottenere regolarmente gli aggiornamenti. Questa funzione è disponibile per tutti i tipi di connessione Internet (Dialup, ISDN, Cable, ecc).

È possibile anche aggiornare manualmente Seqrite Endpoint Security quando necessario, in uno dei seguenti modi:

1. Selezionare **Start > Programmi > Seqrite Endpoint Security > Aggiornamento Rapido**.
2. Seguire le istruzioni e fare clic sul tasto **Avanti**.
3. Selezionare **Scarica da Seqrite Endpoint Security Internet Centre**.
4. Assicurarsi che la connessione Internet sia attiva e poi fare clic su **Avanti** per avviare la procedura di aggiornamento.

5. Aggiornamento Rapido si connette al sito di Seqrite, scarica i file di aggiornamento appropriati e li applica alla propria copia, aggiornandola all'ultimo file di aggiornamento disponibile.

Aggiornare Seqrite Endpoint Security con i file di definizione

Se si possiede il file di definizione per l'aggiornamento, è possibile aggiornare Seqrite Endpoint Security senza connettersi a Internet. È utile per ambienti di rete con più di un sistema. Non è necessario scaricare il file di aggiornamento su tutti i computer dela rete che usano Seqrite. È possibile scaricare gli ultimi file di definizione dal sito di Seqrite da www.seqrite.it.

Per scaricare Seqrite Endpoint Security attraverso il file di definizione, seguire questa procedura:

1. Selezionare **Start** > **Programs** > **Seqrite Endpoint Security** > **Aggiornamento Rapido**.
2. Seguire le istruzioni e fare clic su **Avanti**.
3. Selezionare **Scegli da percorso specifico**.
4. Fare clic su **File** per collocare il file di definizione. Selezionare file .bin.
5. Fare clic su **Avanti**.

Aggiornamento Rapido prende il file di definizione dal percorso designato, ne verifica l'applicabilità sulla versione installata e aggiorna la copia di Seqrite Endpoint Security.

Linee guida per l'aggiornamento ambienti di rete

Seqrite Endpoint Security può essere configurato per fornire aggiornamenti nella rete. Suggeriamo di seguire queste linee guida per avere risultati migliori.

1. Impostare un computer (che potrebbe essere il server) come macchian master per gli aggiornamenti. Supponiamo che il nome del server sia SERVER.
2. Creare una cartella **QHUPD** dove si preferisce. Per esempio: **C:\QHUPD**.
3. Assegnare diritti di sola lettura a questa cartella.
4. Selezionare **Start** > **Programmi** > **Seqrite Endpoint Security** > **Seqrite Endpoint Security** per aprire la Dashboard.
5. Selezionare **Impostazioni** > **Aggiornamento Automatico**.
6. Selezionare **Copia i file nel percorso specificato**.
7. Fare clic su **Sfoglia** e collocare la cartella **QHUPD**. Fare clic su **OK**.
8. Fare clic su **Salva** per salvare questa impostazione.

9. Poi su ogni computer degli utenti, dentro la rete, avviare **Seqrite Endpoint Security**.
10. Andare alla pagina **Aggiornamento Automatico** sotto **Impostazioni**.
11. Selezionare **Prendi i file da percorso speficico.**
12. Fare clic su **Sfoglia**.
13. Collocare la cartella **SERVER\QHUPD** da Risorse di rete. In alternativa è possibile digitare il percorso come **\\SERVER\QHUPD**.
14. Fare clic su **Salva** per salvare le impostazioni.

Pulizia Virus

Seqrite avverte della presenza di un'infezione da virus quando:

- Incorre in un virus durante la scansione manuale.
- Viene trovato un virus dalle funzioni Seqrite Endpoint Security Protezione Virus/Protezione Email.

Eliminare i virus trovati durante la scansione

Le impostazioni predefinite di Seqrite Endpoint Security sono adeguatamente configurate e sono ottimali per proteggere il sistema. Se viene trovato un virus durante la scansione, Seqrite Endpoint Security cerca di ripararlo. Tuttavia, se l'eliminazione del virus fallisce, questo file viene messo in quarantena. Nel caso in cui si siano personalizzate le impostazioni predefinite dello scanner, quando viene trovato un virus prendere i provvediment adeguati.

Opzioni di Scansione

Durante la scansione, vengono fornite le seguenti opzioni per facilitare le operazioni.

Scheda Azioni	Mostra le azioni intraprese sui file.
Salta Cartella	Permette di evitare la scansione della cartella corrente. La scansione si sposta in altre direzioni. Questa opzione è utile durante la scansione di una cartella che contiene elementi non sospetti.
Salta File	Permette di evitare la scansione del fle corrente. Questa opzione è utile durante la scansione di un archivio con un gran numero di file all'interno.
Interrompi	Permette di fermare il processo di scansione.
Chiudi	Permette di uscire dal processo di scansione.
Spegni il PC una volta terminato	Permette di spegnere il sistema alla fine della scansione.

Eliminare i virus trovati nella memoria

“Virus Attivo in memoria” significa che un virus è attivo e che si sta espandendo agli altri file o computer (se connesso a una rete) e sta svolgendo attività malevola.

Quando viene trovato un virus durante la scansione della memoria, viene automaticamente programmato l’avvio di un Boot Time Scan al successivo riavvio del sistema. Il Boot Time Scan effettuerà la scansione e pulirà tutte le unità, incluse le partizioni NTFS, al momento dell’avvio del sistema. Troverà ed eliminerà anche i più difficili rootkits, spywares, trojan con scopi specifici, e logger.

Riavvio necessario durante l’eliminazione di alcuni malware

Durante la scansione dela memoria, quando vengono trovati determianti malware che non possono essere disabilitati o ripuliti, verranno impostati per essere eliminati al successivo. La scansione di memoria di Seqrite Endpoint Security fornirà dettagli o consigli per azioni da intraprendere in questi casi.

Eliminazione di virus Boot/Partition

Nel caso in cui la scansione di memoria di Seqrite Endpoint Security rilevi un boot o partition virus nel sistema, verrà suggerito di riavviare il sistema usando un clean bootable disk e di effettuare la scansione usando Seqrite Emergency Disk per eliminare i virus.

Avvisi in risposta a virus trovati da Protezione Virus

La Protezione Virus di Seqrite Endpoint Security effettua continuamente la scansione del sistema per i virus in background mentre l’utente lavora. Protezione Virus ripara i fie infetti in modo automatico per impostazione predefinita. Ogni volta che la Protezione Virus di Seqrite Endpoint Security avrà intrapreso un’azione si riceverà un messaggio di avviso.

Capitolo 8. Supporto Tecnico

Seqrite fornisce supporto tecnico per gli utenti registrati. Si consiglia di avere tutti i dettagli necessari con voi durante la chiamata per ricevere un supporto efficiente dai responsabili di supporto Seqrite.

Supporto

L'opzione Supporto fornisce un completo supporto online dove è possibile trovare risposta alle proprie necessità e domande in una varietà di modi. Comprende FAQ dove trovare le risposte alle domande più frequenti, opzioni per presentare le vostre domande, per inviare email con le vostre domande, o chiamarci direttamente.

Il Supporto include quanto segue.

Supporto Web

Col Supporto Web, è possibile sottoporre domande, visualizzare le FAQ (Frequently Asked Questions) dove è trovare le risposte alle domande poste più frequentemente. Tuttavia, sarebbe meglio controllare le FAQ almeno una volta, prima di indirizzarsi verso altri mezzi di supporto poichè la risposta alle proprie damande potrebbe essere disponibile nelle FAQ stesse.

Per usare il Supporto Web, seguire questa procedura:

1. Apri **Seqrite Endpoint Security**.
2. Nella barra del menù di Seqrite Endpoint Security, selezionare **Aiuto > Supporto**.
3. Nella schermata di Supporto, fare clic su **Visita FAQ** per visualizzare le FAQ.

   Cercare la risposta alle domande nelle FAQ. Se non si trova una risposta adegata, sottoporre la propria domanda.

Supporto Email

Col Supporto Email, è possibile inviarci una email con le domande così che gli esperti Seqrite possano fornire una risposta appropriata.

Per usare il Supporto Email, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Nella barra del menù di Seqrite Endpoint Security, selezionare **Aiuto > Supporto**.

3. Nella schermata di supporto, fare clic su **Invia Ticket** in **Supporto Email** per sottoporre le domande.

   Facendo clic su Invia Ticket si viene reindirizzati alla nostra pagina web di supporto, dove è possibile sottoporre le domande.

4. È possibile anche richiedere supporto a support@seqrite.com.

Supporto telefonico

Col Supporto Telefonico, è possibile chiamare per ottenre un supporto istantaneo da parte degli esperti Seqrite.

Il segunte è il numero di contatto per il suporto telefonico: +91-9272 21 21 21.

Supporto Remoto

In alcuni casi il Team di Supporto Tecnico Seqrite offre anche supporto remoto. Il Modulo di Supporto Remoto Seqrite permette di connetterci facilmente al sistema del vostro computer attraverso Internet per offrire supporto tecnico da remoto. Ciò ci aiuta a fornirvi un supporto efficiente poichè i nostri esperti possono trovare una soluzione al problema al posto vostro.

Per usufruire del Supporto Remoto, seguire questa procedura:

1. Aprire **Seqrite Endpoint Security**.
2. Nella barra del menù di Seqrite Endpoint Security, selezionare **Aiuto** > **Supporto**.
3. Fare clic su **Supporto Remoto**.

   Si apre la schermata con termini del contratto per il Suporto Remoto.

4. Fare clic su **Accetto**.
5. Fornire l'**ID** disonibile nell'agent del Supporto Remoto Seqrite al team di supporto esecuitvo Seqrite.

   Vengono visualizzati i dettagli per l'accesso remoto come l'indirizzo IP e l'ID di accesso remoto. Fornire questi dettagli agli ingegneri del supporto remoto che si collegheranno così al vostro sistema. Il Supporto esecutivo Seqrite accederà al sistema da remoto per risolvere il problema.

Supporto Live Chat

Col Supporto Live Chat, è possibile effettuare una sessione in chat con i responsabili tecnici Seqrite.

Supporto Tecnico

Quando è il momento migliore per chiamare?

Quick Heal Technologies (P) Ltd. fornisce supporto tecnico tra le 9:30 e le 18:30, dal Lunedì al Sabato IST (Tempo Standard Indiano).

Quale numero chiamare?

Gli utenti possono chiamare il numero +91 - 92722 12121.

I dettagli che sono necessari durante la chiamata sono:

- Il Product Key che è incluso nella scatola prodotto. Se il prodotto è stato acquistato online, la chiave prodotto è stata inviata nell'e-mail di conferma dell'ordine.
- Le informazioni relative al computer: marca, tipo di processore, capacità della RAM, dimensione del disco rigido e lo spazio libero su di esso, così come informazioni su altre periferiche.
- Il sistema operativo: nome, numero versione, lingua.
- Versione dell'antivirus installata e data del database dei virus.
- Software installato sul computer.
- Il computer è collegato a una rete? Se sì, contattare prima gli amministratori di sistema. Se gli amministratori non possono risolvere il problema devono contattare il supporto tecnico Seqrite.
- Dettagli: Quando si è verificato il problema per la prima volta? Cosa stavate facendo quando il problema è apparso?

Molto spesso, questa informazione ci aiuta a risolvere il problema velocemente.

Cosa dire al personale tecnico di supporto?

Dovrete essere il più specifici possibile e fornire i minimi dettagli di cui il supporto esecutivo avrà bisogno per fornire una soluzione sulla base delle vostre indicazioni.

Global Support Center

Supporto telefonico: +91–92722–33000.
Email: support@seqrite.com

Contatto Quick Heal Technologies

Head Office

Quick Heal Technologies (P) Ltd.

603, Mayfair Towers II,

Wakdewadi, Shivajinagar,

Pune 411 005, Maharashtra

Email: support@seqrite.com

Per maggiori dettagli visitare: www.seqrite.com.

Contatto Distributore per l'Italia Quick Heal Technologies

netWork Sas

Via E. Spinucci, 39/41

50141 Firenze

Email: info@seqrite.it

Per maggiori dettagli visitare: www.seqrite.it